MEGI

MESTRADO
Estatística e Gestão de Informação

Análise ao processo de gestão de palavras-chave num sistema informático e riscos inerentes

Estudo de um sistema numa instituição de seguros no Mercado português

António Luís Lima Fernandes

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Estatística e Gestão de Informação

UNIVERSIDADE NOVA ISEGI

Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

ANÁLISE AO PROCESSO DE GESTÃO DE PALAVRAS-CHAVE NUM SISTEMA INFORMÁTICO E RISCOS INERENTES: ESTUDO DE UM SISTEMA NUMA INSTITUIÇÃO DE SEGUROS NO MERCADO PORTUGUÊS

por

António Luís Lima Fernandes

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Estatística e Gestão de Informação, Especialização em Análise e Gestão de Risco

Orientador: Professor Doutor Rui Gonçalves

novembro 2014

AGRADECIMENTOS

Em primeiro lugar, agradeço ao CEO da empresa onde trabalho e à minha Diretora, por me terem permitido efetuar este trabalho com a informação da companhia. De igual modo, quero agradecer ao meu superior hierárquico por me ter apoiado neste trabalho e ajudado no envio do inquérito aos colegas da empresa.

Também quero agradecer ao meu orientador, Professor Rui Gonçalves, por ter achado este tema interessante e pela sua disponibilidade para me ajudar sempre que solicitei a sua ajuda.

Agradeço à professora Jennifer Lã, pela ajuda que me deu ao corrigir o Abstract deste documento e às lições que me ensinou ao analisar o documento.

Quero também agradecer ao meu pai por me ter incentivado a realizar este trabalho e a lembrar-me constantemente que a Segurança da Informação, quando é digital, nunca existe a 100%, pois existem brechas nos esquemas de segurança, propositados ou não, que fazem com que os nossos dados circulem entre desconhecidos com os mais variados propósitos.

Deixo aqui uma palavra de agradecimento ao meu irmão Pedro, pelas horas que poderia estar no computador e que perdeu enquanto realizei o trabalho.

Por fim, agradeço à Catarina pela paciência que teve pelas horas em que não estive com ela e por me ter incentivado a acabar este trabalho. Não deixo de agradecer também por me ter ajudado a encontrar o tema, enquanto estava à procura.

RESUMO

Os maiores ativos de uma instituição seguradora são os dados dos clientes, pois através destes as políticas e objetivos da empresa são planeados e alargados. Esses dados são considerados críticos ou confidenciais, como o caso de nomes, moradas, dados de saúde e sinistros, que devem ser protegidos contra ameaças internas (fraude, erros de utilização) e externas (roubo de informação). A fuga de informação representa graves perdas de uma instituição, cujos danos vão desde perda de reputação ao afastamento de clientes, parceiros e até mesmo colaboradores, processos jurídicos e danos financeiros. Assim, a utilização de palavras-passe fortes, com regras rígidas para a sua gestão, do conhecimento de toda a empresa é importante para manter a Segurança da Informação.

Regra geral, para um colaborador autorizado a consultar determinada informação entrar nessas bases de dados, autentica-se através da inserção de um Nome de Utilizador e de uma Palavra-passe num sistema. A gestão de palavras-chave insere-se no Risco Operacional, associado às atividades diárias de uma organização, envolvendo processos, pessoas e sistemas, que hoje em dia é considerado importante para uma gestão empresarial saudável e não apenas todo o risco não quantificável, como era considerado há alguns anos atrás.

O objetivo deste trabalho será analisar o processo de gestão de palavras-chave numa seguradora a atuar em Portugal, ou seja, que processos e regras a empresa tem para que os seus colaboradores criem as suas palavras-chave. Será também analisado as ameaças que os sistemas de palavras-passe enfrentam, no geral, e verificar-se-á de que maneiras esta organização protege-se dessas ameaças e como será possível mitigar os riscos existentes, através da melhoria dos processos existentes ou da implementação de novas soluções.

PALAVRAS-CHAVE

Palavras-passe; Risco; Risco Operacional; Segurança da Informação; Proteção

ABSTRACT

Customer data are the greatest assets of an insurance institution, because through these, policies and objectives of the company are planned and designed. These data, together, are often considered critical or confidential as is the case of names, addresses, health data and claims. These must be protected against threats, both internal (fraud and misusage) and external (data theft). Leakage of information is a serious loss for an institution. The damage causes ranges from loss of reputation to the defection of customers, partners and even employees, as well as to lawsuits and financial losses. Thus, using strong passwords, with strict rules for their management, which the entire company knows, is important for maintain information security.

Generally, for an employee authorized to consult certain information, to access those databases, he/she authenticates him/herself through the insertion of a Username and a Password. Password management is not just any unquantifiable risk, as it was considered a few years ago: it is part of the Operational Risk associated with the daily activities of an organization, involving processes, people and systems, which nowadays are considered important for a healthy business.

The objective of this work is to analyze the process of managing passwords in an insurance company to act in the Portuguese market, i.e., rules and processes that the company has for its employees to create their passwords. The threats that systems of passwords face in general will also be reviewed, and the ways that this organization protects itself from these threats will be studied. Finally, how the organization can mitigate the risks by improving existing processes or implementing new solutions will be discussed.

KEYWORDS

Passwords; Risk; Operational Risk; Information Security; Protection

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

APAC Asia-Pacific. Região do mundo que inclui a Ásia oriental, sul da Ásia, sudeste da Ásia e a Oceânia

ASCII American Standard Code for Information Interchange. Código binário que codifica caracteres, utilizado para representar texto em computadores

EIOPA European Insurance and Occupational Pensions Autorithy. Autoridade europeia de seguros e pensões complementares de reforma

EMEA Europe, the Middle East and Africa. Região que engloba a Europa, o Médio Oriente e África

ISMS Information Security Management System. Em português significa Sistema de Gestão da Segurança da Informação

ISO International Organization for Standardization. Entidade que aprova normas internacionais em todos os diferentes campos

IT Information Technology. São as Tecnologias de Informação, ou seja, o conjunto de atividades e soluções providas por recursos tecnológicos cujo objetivo é a produção, armazenamento, transmissão, acesso, segurança e uso das informações

NIF Número de Identificação Fiscal. É o número de contribuinte, pessoal a cada cidadão, que serve ao tratamento de informação de índole fiscal

PIN Personal Identification Number. É um número de identificação pessoal, numérico, para autenticar um utilizador num sistema

1. INTRODUÇÃO

Um sistema de palavras-chave para aceder a determinado conteúdo é comum em todo o mundo (Pogue, 2011). Basta verificar que, para aceder a uma conta no banco, precisa-se de um código, para garantir que ninguém acede ao dinheiro dos outros. Para aceder ao email, é necessária uma senha de acesso para que estranhos não leiam as mensagens de outrem.

Deste modo, a privacidade de um indivíduo é garantida, pois existe uma barreira que impede que pessoas indesejadas possam aceder à informação para uso próprio ou mesmo roubar a identidade desse indivíduo, para atos ilícitos (Solove, 2003).

Para garantir que a gestão das palavras-passe seja eficaz dentro de uma organização, é necessário que esta tenha uma boa política de Segurança da Informação para gerir os riscos que posam ocorrer e proteger a sua informação (Santos & Silva, 2012). Afinal de contas, numa economia moderna, a Informação é considerada o seu sangue (Thomson & von Solms, 2005).

A Segurança da Informação está relacionada com IT, uma vez que grande parte da Informação que circula numa empresa está inserida em plataformas tecnológicas, pelo que grande parte de autores, como Grob et al. (2008) ou Savić (2008) consideram que o risco tecnológico é um risco que se tem quando a informação é alterada, acedida ou utilizada por indivíduos sem permissões para tal e, consequentemente, quanto maior a quantidade de informação que uma organização tem em seu poder, maior são os problemas que podem ocorrer. Deste modo, será necessário as organizações identifiquem e classifiquem os seus dados mais importantes, para determinarem o seu nível de segurança (Burg et al., 2014). A Segurança da Informação deverá garantir que a informação existente está protegida (Santos & Silva, 2012), ou seja, que esta mantenha as suas características: confidencialidade, integridade e disponibilidade (Benaroch et al., 2012).

A questão da segurança da Informação numa companhia de seguros é importante, uma vez que existe muita informação considerada sensível a circular nos seus servidores que não deve ser roubada ou cair no conhecimento público, como dados pessoais (nomes, moradas, telefones), dados de sinistros (danos materiais, veículos), dados médicos (lesões, incapacidades, despesas médicas, cirurgias) ou até uma combinação dos três tipos de informação (Daniel, 2009).

Uma quebra na segurança da informação de uma empresa caracteriza-se como pertencente ao Risco Operacional, sendo o único inerente à companhia (Jarrow, 2008),

entre todos os tipos de risco (incluindo o risco de mercado, crédito e liquidez) associados a uma organização. O Risco Operacional resulta na falha ou inadequação de processos internos (Gillet et al., 2010), tais como fraude, roubo, terrorismo, vandalismo ou desastres naturais (Gonçalves, 2011).

Uma falha na proteção da informação pode levar a uma quebra na reputação da organização, o que leva a uma perda no valor da firma (Jarrow, 2008). Assim, será necessário que essa mesma empresa tenha uma gestão de risco que possa identificar, analisar e avaliar os riscos que enfrenta, para os combater ou, pelo menos, minimizá-los. Neste caso, risco não representa perigo, ou consequências negativas como normalmente é associado (Leitch, 2010), mas um efeito de incerteza nos objetivos.

Portanto, uma falha relacionada com a gestão de palavras-chave, que pode levar à perda reputacional de uma organização é um risco que as empresas têm de analisar e combater, sob pena que os seus objetivos corporativos sejam comprometidos.

1.1. RELEVÂNCIA DO TEMA

A utilização de palavras-passe é das formas mais comuns de autenticação em todo o mundo (Sandhu & Samarati, 1996), o que permite ao utilizador aceder a uma parte específica de um sistema. Uma vez que esta é uma porta de entrada para os sistemas e como a informação cada vez mais é digital (Thomson & von Solms, 2005), com acesso praticamente ilimitado e imediato à informação (Almaça, 2010), grande parte dos ataques informáticos visa a descoberta das palavras-chave para aceder a informações confidenciais.

Algumas das notícias recentes mostram que este campo sofre diversos ataques que podem comprometer seriamente algumas empresas, como o caso em que piratas informáticos roubaram mais de 500 milhões de contas de correio eletrónico, incluindo empresas que estão na lista da Fortune 500[1]. O *heartbleed bug* é outro exemplo de ataque, que devido a uma falha nos sistemas de criptografia dos servidores de uma série de empresas, permitiu que piratas informáticos roubassem as palavras-passe e os nomes de identificação[2].

[1] Retirado de http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html, visitado a 18 de novembro de 2014

[2] Retirado de http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/, visitado a 18 de novembro de 2014

Segundo a Verizon (2013), quatro em cada cinco falhas reportadas estão relacionadas com roubos de credenciais de autenticação (conhecido como *password dumper*). Esta técnica está dentro das vinte principais ações maliciosas, sendo inclusivamente utilizadas para efeitos de espionagem. Estes roubos afetam principalmente a América, seguido da EMEA e, por último, a APAC. Ainda segundo van Osten (2014), 76% de todas as intrusões tem como objetivo explorar ou roubar credenciais. Solove (2003) escreve que, por ano, existem meio milhão de roubos de identidade.

Entre os tipos de ataques mais comuns, destacam-se três: ataques de dicionário, em que o hacker[3] tenta introduzir palavras conhecidas para aceder à informação confidencial; força bruta, em que se tenta aceder aos dados do utilizador através do método de tentativa e erro até encontrar as credenciais corretas; *honey pot attack*, em que o pirata informático visa entrar no servidor que aloja as credenciais de acesso para recolher essa informação (Acar et al., 2013).

Assim, uma boa política de Segurança da Informação que obrigue as empresas a terem uma série de normas obrigatórias na definição e utilização de senhas de autenticação, é importante para protegerem os seus dados contra ataques de hackers. Por exemplo, uma regra simples é obrigar os utilizadores criarem palavras-chave com alguma complexidade, para não criarem palavras-chave demasiado simples, como as que o SplashData[4] divulga anualmente, que são mais suscetíveis de serem descobertas.

Na ótica de uma seguradora, o comprometimento das palavras-passe pode implicar uma perda de informação que responsabiliza a gestão da organização bem como a reputação da mesma (Gillet et al., 2010). A informação de uma seguradora pode ser dividida em duas áreas:

- Dados pessoais dos segurados: nome, morada, NIF, contactos, matrículas de automóveis, dados clínicos, lesões, local de trabalho (Daniel, 2009)
- Dados da organização: salários, comissões, gastos correntes, lucros, dados dos colaboradores, mediadores, resseguradores (Horta, 2014)

Consoante a informação for mais crítica para a seguradora, maior será o controlo que terá de efetuar para manter essa informação segura. São casos de medidas como controlos de acessos de rotina, encriptação, autenticação multifator, autenticação biométrica, chaves longas, entre outras.

[3] Pirata informático
[4] Empresa dos EUA que providencia aplicações e serviços de segurança informática

Horta (2014) defende que, para uma gestão saudável de uma seguradora, os colaboradores devem privilegiar o uso do email para se contactarem entre si, uma vez que nesta plataforma a informação fica registada e disponível, mesmo que o recetor se esqueça ou seja transferido ou demitido do seu lugar. Segundo o autor, "o que não se escreve não existe".

1.2. OBJETIVO

O objetivo desta dissertação é efetuar a análise ao processo de gestão de palavras-chave de um sistema numa seguradora a atuar em Portugal, tendo em conta a importância dos dados e da informação que a empresa guarda nos seus sistemas e dos perigos que podem advir caso os mesmos fossem roubados.

Para ajudar a alcançar este objetivo foram definidos os seguintes objetivos específicos:

- Descrição do processo de gestão de palavras-chave num sistema da organização em estudo;
- Identificação dos principais riscos que o processo pode ter;
- Verificação dos pontos de controlo implementados para mitigar os possíveis riscos;
- Análise de novos métodos de mitigação do risco no processo em causa.

Estes objetivos específicos podem dividir-se em duas áreas. A primeira prende-se com a análise à organização em estudo, ou seja, analisar-se-á como esta gere as suas senhas de acesso para a utilização dos seus colaboradores e quais as regras com que se rege para maximizar a proteção das palavras-passe.

A segunda área é um estudo mais direcionado para fora da organização. Por um lado, verificar-se-á que riscos e problemas as senhas de acessos enfrentam, e por outro, que soluções existem para melhorar a segurança da informação através das palavras-passe.

2. REVISÃO BIBLIOGRÁFICA

2.1. RISCO

A palavra risco, tal como se conhece hoje, não teve o mesmo significado ao longo dos séculos nem das regiões. De facto, não existe uma precisão de quando a palavra risco foi usada nem qual o seu significado (Aven, 2012), embora se defenda que advém do árabe "risq", que significava "o que foi dado por Deus e que retiras proveito" (Althaus, 2005). De seguida, apresenta-se uma tabela com alguns dos significados que a palavra risco teve ao longo dos anos. Apesar do significado de risco ser variável, pode-se verificar que alguns dos significados mais comuns associados a este conceito é "sorte", "conflito" ou "perigo".

Local	Termo	Época	Significado
França	Risqué	1578	Perigo; inconveniência
Itália	Risco	Século XIV (1ª metade)	Possibilidade de dano; consequência desagradável
Latim pós-clássico	Resicum, risicum	Meados século XII	Perigo
Francês médio	Resicq; risicq	Século XV (2ª metade)	Perda ou dano na mercadoria
Occitânico[5] antigo	Rezegue	1200	Possibilidade de perda ou dano da mercadoria transportada por mar
Catalão	Risc, reec	Século XIII	Possibilidade de perda ou dano da mercadoria transportada por mar
Espanhol	Riesgo	1300	Conflito, desacordo
Dutsch	Risico; resicq; risicque	De 1525 a 1602	Possibilidade de perda na mercadoria
Árabe	Rizq	Época medieval	Fortuna, sorte, destino, chance

Tabela 1 – Significados da palavra "risco" ao longo do tempo
Fonte: Aven (2012)

[5] Língua românica falada no sul de França

Atualmente, o conceito de risco é definido comummente como sendo a probabilidade ou a possibilidade de perda ou dano (Brinkmann, 2013), ou como incerteza (Aven, 2012), (Leiss, 2010). Embora certos autores associem o conceito de risco a perigo (Nichols, 2000), outros como Merkelsen (2011) defendem que risco não deve estar relacionado com perigo. Por outras palavras, o risco está associado às decisões tomadas pelos indivíduos, ao passo que o perigo está relacionado com fatores externos.

Segundo a Figura 1, embora os conceitos de risco e perigo sejam semanticamente diferentes, ainda podem ser utilizados como sinónimos (zona a cinza). Por exemplo, segundo Zsidisin (2003), o risco pode ser o perigo que eventos ou decisões poderão obstruir a organização de alcançar os seus objetivos. Contudo, risco não deve ser apenas conotado com aspetos negativos, como perigo ou exposição. Pode ser positivo, como "ter sorte de" ou "tirar proveito de" (Althaus, 2005), embora a maior parte dos indivíduos prefira tomar mais riscos para evitar uma perda que a possibilidade de obter um ganho (Nichols, 2000).

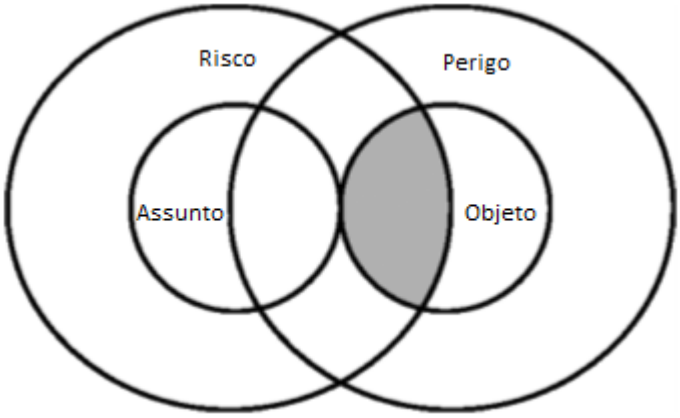


Figura 1 – Semântica de Risco e Perigo
Fonte: Merkelsen (2011)

Atualmente, como verificado, o conceito de risco é variável, de acordo com o ambiente em que se encontra (Aven, 2012) e a perspetiva dos indivíduos (Zsidisin, 2003). Assim, de acordo com os estes e a sua experiência ou conhecimento, as ações a tomar para se prevenirem face ao risco também é diferente (Merkelsen, 2011).

Conforme a Tabela 2, verifica-se que, de acordo com a área, a sua perceção e conhecimento aplicado face ao desconhecido é diferente para cada situação. Ainda

segundo Aven (2013), a definição do conceito de risco é baseada nos julgamentos das pessoas.

Disciplina	Como perceciona o risco	Conhecimento aplicado ao desconhecido
Lógica e Matemática	Risco como fenómeno calculado	Cálculo
Ciência e Medicina	Risco como realidade objetiva	Princípios, postulados e cálculo
Antropologia	Risco como fenómeno cultural	Cultura
Sociologia	Risco como fenómeno social	Construções sociais ou frameworks
Economia	Risco como fenómeno decisor, significado de segurança saúde ou evitar perdas	Princípios de tomada de decisão e postulados
Jurídico	Risco como falta ou conduta e fenómenos jurídicos	Regras
Psicologia	Risco como fenómeno comportamental e cognitivo	Conhecimento cognitivo
Linguística	Risco como conceito	Terminologia e significados
História e humanidades	Risco como história	Narrativas
Artes	Risco como fenómeno emocional	Emoção
Religião	Risco como ato de fé	Revelação

Tabela 2 – Diferenças na perceção do risco e no desconhecido para as diferentes disciplinas
Fonte: Althaus (2005)

Com todos estes conceitos e variações de risco, a ISO apresentou uma diretiva (ISO 31000:2009) para clarificar e estandardizar este conceito, para evitar que cada entidade efetuasse a sua interpretação do risco e a adaptasse para cumprir os seus objetivos (Purdy, 2010). Assim, de um modo conciso, risco pode ser definido como "efeito da incerteza nos objetivos" (Aven, 2013). Aqui, o conceito de incerteza é o conjunto de fatores que ameaçam o alcançar dos objetivos, sejam negócios, circunstâncias ou eventos, que podem ser classificados por componente (o que pode

acontecer), probabilidade (até quanto pode acontecer) e consequência (custo). Deste modo, um evento pode ser mensurável e comparado com outros.

O mesmo documento da ISO31000:2009 incluiu, para ajudar na gestão e uniformização do conceito de risco, uma lista com os termos e definições utilizados na gestão do risco; princípios da gestão do risco; a descrição do processo da gestão do risco e uma descrição dos processos de gestão para alguns riscos específicos (Leitch, 2010).

Conforme indicado na Figura 2 a gestão do risco passa essencialmente por identificar, analisar e avaliar o risco (Luko, 2013). No final, caso a avaliação do risco seja desfavorável, deve-se proceder para minimizar o mesmo. Se existir mais que uma solução, a escolhida deverá ser aquela que tem melhor relação custo-benefício (Leitch, 2010).

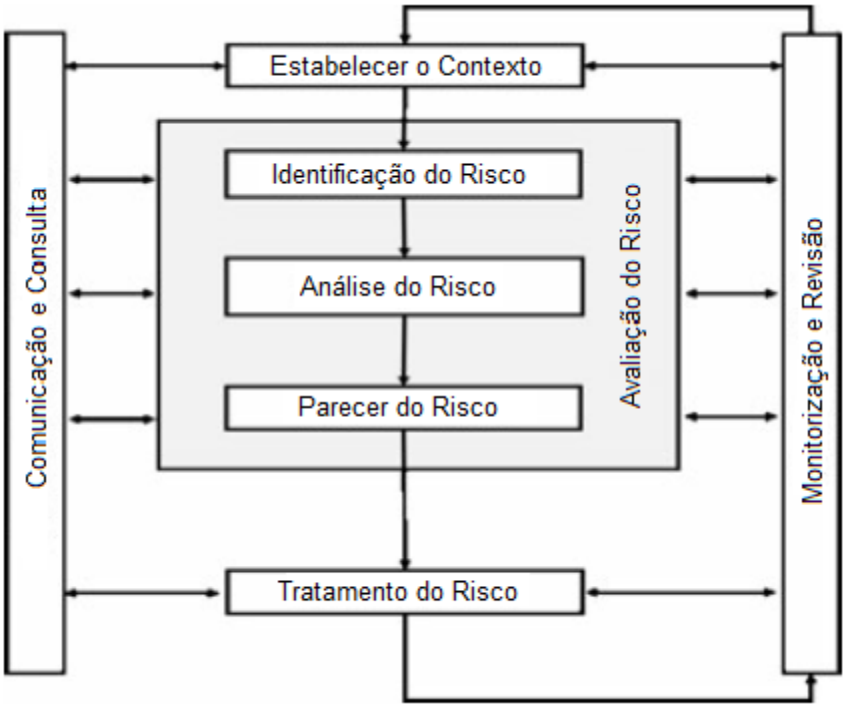


Figura 2 – Gestão do Risco
Fonte: Purdy (2010)

Enquanto que a ISO31000:2009 foca-se na gestão do risco, a ISO27000 está direcionada para a Segurança da Informação (Disterer, 2013). Esta última considera risco como "combinação da probabilidade de um evento e das suas consequências" (Santos & Silva, 2012) e risco de Segurança da Informação como "potencial que uma

ameaça explore uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à organização".

Para contrariar estas ameaças, a ISO27000 recomenda a criação de um Sistema de Gestão de Segurança de Informação (ISMS, no original) cujo objetivo primordial é salvaguardar a confidencialidade, integridade e disponibilidade da informação (Standardization & Commission, 2013), através da criação de um modelo para controlar, monitorizar e melhorar a proteção destes ativos (International Organization for Standardization, 2009). Tal só poderá ser feito através da análise ao risco, conforme referida na ISO31000.

2.2. RISCO OPERACIONAL

A gestão do risco divide-se em quatro tipos de risco: risco de mercado, risco de crédito, risco de liquidez e risco operacional (Jarrow, 2008). Segundo Sturm (2013), apenas na última década este último risco tem atraído mais atenção por parte dos reguladores e entidades.

Originalmente, o Risco Operacional era definido como "todo o tipo de risco não quantificável enfrentado por um banco" (Savić, 2008). A definição, segundo o EIOPA (CEIOPS, 2009), é "o risco de perdas resultante da inadequação ou falhanço de processos internos, pessoas e sistemas, ou de eventos externos. Esta definição inclui risco legal, mas exclui os riscos estratégicos e reputacional". Ou seja, este tipo de risco está relacionado com as atividades diárias de uma organização, gestão, processos, entre outros.

O risco operacional pode ser dividido em duas partes: custos de agência (como por exemplo fraude e problemas de produção) e riscos tecnológicos/sistema (Jarrow, 2008). Precisamente, quando a exposição a Tecnologias de Informação e à automação é superior, o risco operacional aumenta (Sturm, 2013). Corroborando o primeiro parágrafo, Savić (2008) diz que o risco de IT, há pouco tempo atrás, ocupava uma posição baixa no Risco Operacional, embora o aumento da informação tecnológica represente um maior risco para a organização (Grob et al., 2008).

Como se pode verificar na Tabela 3, os Riscos Operacionais relacionados com IT dividem-se em três pontos-chave:

Confidencialidade: Os dados são apenas acedidos a quem está devidamente autorizado para consultar os mesmos e o sistema encontra-se protegido contra

ataques de *phishing*[6] ou de hackers. Os dados podem ser considerados organizacionais (planos estratégicos da organização) ou privados (como dados médicos de clientes).

Integridade: Garantir que os dados são autênticos, genuínos e encontram-se preservados sem corrupção. Neste ponto, deve-se garantir que estes estão protegidos contra atos de vandalismo ou de erro humano que possa comprometer a informação.

Disponibilidade: Os dados estão acessíveis no menor tempo possível a quem necessita dos mesmos. Isto implica que os dados devem estar disponíveis mesmo em caso de ataques, erros, problemas técnicos ou catástrofes naturais.

Alvo	Exemplos de eventos de Riscos Operacionais em IT
Confidencialidade	Roubo do código fonte proprietário
	Empregado perde bloco de notas com dados sensíveis da empresa
	Indivíduo de fora obtém senhas através de phishing e rouba recursos de clientes
	Companhia posta, por erro, dados pessoais de clientes no site público
	Uso não autorizado de códigos de acesso e palavras-chave por pessoas internas
Integridade	Hacker penetra em contas de corretores e efetua trocas não autorizadas
	Alimentação de dados errados causa transações liquidadas a preços incorretos
	Rede de ATM exibe comportamento defeituoso por causa de um erro de software
	Alguém de fora da companhia entra e desfaz o site da companhia
	Banco entra numa troca comercial incorreta devido a um erro de teclas de um comerciante
Disponibilidade	Ataque de Negação de Serviço
	Sistema de negociação falha devido a um disco rígido defeituoso
	Reprodução de vírus sobrecarregam os servidores de largura de banda de rede e email
	Site não recebe encomendas de clientes por causa de um problema de ISP

Tabela 3 – Exemplos de eventos de Riscos Operacionais em IT
Fonte: Benaroch, Chernobai & Goldstein (2012)

De modo a evitar problemas relacionados com o Risco Operacional, com especial enfoque no Risco de IT, foi criada a norma ISO27000, que pretende normalizar criar normas para a proteção dos sistemas de IT (Disterer, 2013; Georg, 2013), uma vez que problemas nesta área afetam negativamente a reputação da empresa (Jarrow, 2008).

Esta norma pretende realçar a importância do planeamento, implementação e de melhorias para a proteção contra este risco, bem como destacar a importância da monitorização e verificações constantes aos sistemas, para reforçar a segurança. Esta ISO pretende, para além de estandardizar as normas, certificar as empresas que

[6] Tentativa de adquirir dados pessoais, através da imitação de empresas ou pessoas confiáveis, como bancos ou empresas de distribuição

cumpram estes requisitos, o que permitirá aumentar a reputação das mesmas (Disterer, 2013).

2.3. SEGURANÇA DA INFORMAÇÃO

O risco de IT aumenta de acordo com a dependência das organizações e dos indivíduos nas tecnologias (Santos & Silva, 2012), pelo que, quanto maior for a informação guardada nos sistemas, maior é o risco de ocorrer uma falha (Grob et al., 2008).

Com o surgimento do comércio eletrónico, com base em computadores e telecomunicações em todo o processo de negócio, apareceram novas questões de segurança (Dutta & McCrohan, 2002), para a proteção da informação criada, adquirida e guardada nos sistemas, contra a utilização maliciosa da informação ou o roubo deste (Astakhova, 2014). Os alvos mais apetecíveis são a informação sensível e valiosa, especialmente de empresas do setor financeiro e de outras entidades críticas (Burg et al., 2014).

2.3.1. Informação

Antes de avançar com o conceito de Segurança da Informação, é necessário definir o que é a informação e qual a sua importância para as organizações. Grande parte dos autores considera a informação como um ativo organizacional (Thomson & von Solms, 2005), que pode ser armazenada e transmitida de muitas formas (International Standard Organization, 2009). Por vezes é considerada uma imagem subjetiva do mundo (Astakhova, 2014), numa visão mais científica.

Num contexto empresarial, a informação é o sangue da economia eletrónica, que deve ser gerida, controlada (Thomson & von Solms, 2005) e protegida, tal como os seus elementos críticos tais como sistemas, software ou hardware (von Solms & van Niekerk, 2013).

Dependendo da classificação que cada empresa atribui à sua informação, os processos de controlo também variam. Por exemplo, a informação pública, como a que está publicada no site de empresa não necessita de nenhum controlo especial, uma vez que se trata de informação que pode ser partilhada fora da organização. No outro extremo, está a informação secreta (ou restrita), cuja divulgação está disponível somente a um número reduzido de colaboradores internos, mediante autorização.

Esta informação tem maiores sistemas de segurança como encriptação, palavras-chave fortes e/ou longas ou autenticação biométrica.

Como a informação é substancialmente digital, normalmente o risco de IT está relacionado com a utilização da informação numa organização (Grob et al., 2008), ou seja, a informação ser acedida, alterada ou utilizada por indivíduos sem direito a tal (Savić, 2008), por ataque, por erro, ou mesmo por causas naturais como por exemplo, incêndios nos servidores (International Standard Organization, 2009).

2.3.2. Segurança da Informação

A Segurança da Informação é a preservação da confidencialidade, integridade e disponibilidade da informação, sob várias formas (Anderson, 2003). Por outras palavras, é a proteção da informação e também dos seus elementos críticos, como sistemas, software, ou hardware (von Solms & van Niekerk, 2013). Segundo a Federação Russa, a definição de Segurança da Informação é o estado de proteção dos interesses nacionais na esfera da informação, determinados pelos equilíbrios dos interesses individuais, sociais e da nação (Astakhova, 2014).

A Segurança da Informação tem de ser uma decisão tomada pela organização como parte da estratégia, de acordo com os seus objetivos e necessidades (Standardization & Commission, 2013), pelo que não se trata de um produto, mas de um processo (von Solms & van Niekerk, 2013). Esse processo contém uma série de regras e procedimentos que devem ser seguidos de acordo com as necessidades e tarefas dos colaboradores de uma organização (Ellwanger et al., 2012).

Deste modo, como a informação é um ativo importante para as organizações, que corre sérios riscos de ataques, é necessário que as organizações implementem planos de Segurança da Informação, para minimizar o impacto. Impacto esse que é difícil de se medir, pois pode implicar desde roubos de dados (como cartões de crédito) até à própria satisfação dos clientes (Dutta & McCrohan, 2002) e publicidade da empresa (Anderson, 2003). Neste último caso, pode-se verificar que 44% das organizações que sofreram ataques informáticos tiveram impactos financeiros (Dutta & McCrohan, 2002).

Na área dos seguros, segundo o documento publicado por Burg et al. (2014), e conforme o gráfico 1, embora 38% das respostas indicaram que não houve incidentes relacionados com a segurança eletrónica, os ataques foram sobretudo comprometimento ou roubo de dados confidenciais, dados de clientes, fraude e acessos não autorizados.

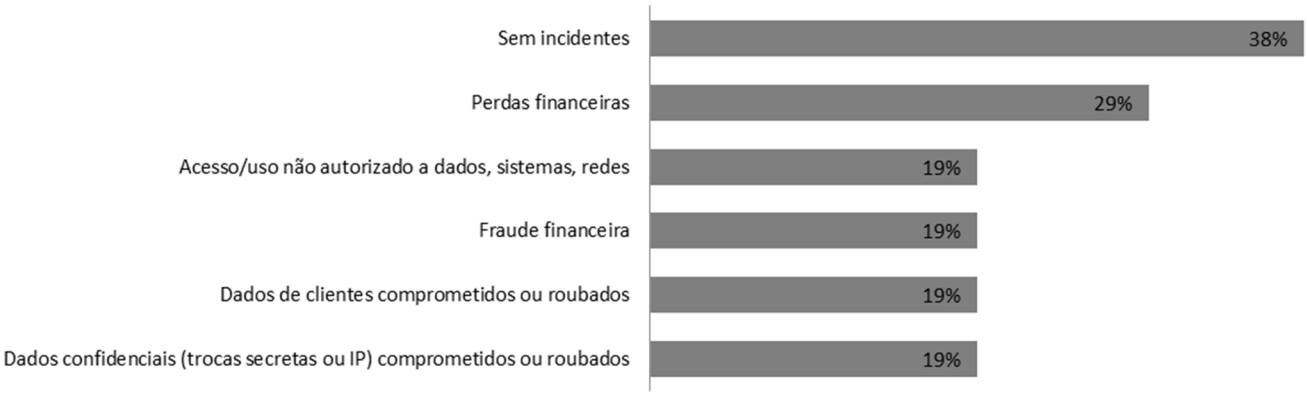


Gráfico 1 – Incidentes significativos detetados na indústria seguradora
Fonte: Burg et al. (2014)

2.3.3. Abordagens da Segurança da Informação

Regra geral, a Segurança da Informação é tratada como uma sobrecarga nas organizações. Por exemplo, no Reino Unido, 27% das empresas gastam menos de 1% dos recursos alocados para IT na Segurança da Informação (Thomson & von Solms, 2005). Muitas organizações ainda pensam que a Segurança de Informação é algo técnico que apenas as áreas de Informática se deverão preocupar (von Solms & von Solms, 2004), ou que basta ter o software atualizado para manterem-se seguros (van Osten, 2014).

A Segurança da Informação deve obedecer a alguns critérios específicos, para que seja mais eficaz contra ataques (espionagem, vandalismo) ou problemas de outro género (fraudes, causas naturais). Para tal, cada organização deve ter presente uma Política de Segurança de Informação (Ellwanger et al., 2012), com procedimentos e regras que os colaboradores devem ter presente. Refere-se já aqui que a simples compra de software não resolve o problema e a proteção da informação acarreta custos e pode inclusive reduzir a eficiência dos sistemas (Dutta & McCrohan, 2002). Seguidamente apresentam-se três caminhos para a Segurança da Informação, cada um envolvendo um meio diferente.

2.3.3.1. Tecnológico

A Segurança da Informação deve ter em atenção a tecnologia utilizada nas organizações, pois é com base nestes sistemas que a Informação é armazenada e circulada, pelo que a dependência de IT nas organizações é elevada (Benaroch et al., 2012). Assim, segundo Chen et al. (2011), é necessário que:

a) Invista-se em tecnologia de segurança para impedir ataques
b) Diversifique-se o software utilizado dentro da empresa para limitar ataques correlacionados
c) Invista-se em IT para reparar as falhas após os ataques

Assim, uma empresa que cumpra estes passos, está a precaver-se dos ataques, bem como a estar apta a responder e a retomar o normal curso após algum problema. Os ataques podem ser propositadamente causados por hackers, invasores, criadores e disseminadores de vírus, ou acidentalmente por defeitos técnicos, falhas de hardware e software (Santos & Silva, 2012).

Sobre o investimento em tecnologia de segurança para impedir ataques, Melro et al. indicam que é necessário manter atualizadas as técnicas e procedimentos, desde que se conserve a relação custo-benefício, embora Thomson & von Solms (2005) indiquem que o investimento em Segurança da Informação é considerado como um fardo para as empresas. O relatório da Verizon 2014 PCI Compliance Report (van Osten, 2014) indica que ter apenas o software atualizado não é o suficiente para manter a segurança da organização.

O segundo ponto, sobre a diversificação de software é, talvez, o ponto mais divergente dentro das organizações. Por um lado, se uma companhia utilizar o software do mesmo fornecedor, permite a compatibilidade e a interoperabilidade entre os sistemas, reduzindo as economias de escala. Por outro lado, a organização fica sujeita a ataques que afetam os sistemas mais populares, tal como os parceiros de negócio que possam utilizar o mesmo software. Pode também ser afetada em múltiplos sistemas, o que aumenta o prejuízo. Assim, a escolha de software deve ser ponderada colocando estes dois pratos na balança, de modo a conseguir um equilíbrio.

2.3.3.2. Processual

Segundo a ISO27000, as organizações devem ter um Sistema de gestão de Segurança da Informação, sendo este um modelo para estabelecer e melhorar a proteção da Informação para alcançar os objetivos corporativos. Para tal, precisam de seguir os seguintes passos:

a) Monitorizar a avaliar os controlos e procedimentos existentes;
b) Identificar possíveis riscos;
c) Escolher, implementar e melhorar os controlos, em função dos riscos identificados

Esta gestão deve estar expressa em políticas de segurança de Informação, bem como standards, procedimentos e guiões, aplicados em toda a organização. Estes passos devem estar de acordo com as necessidades da empresa e precisam de estar escritos numa linguagem clara e simples, para facilitar a comunicação.

Uma maneira de escolher os melhores processos será seguir as melhores práticas disponibilizadas internacionalmente (von Solms & von Solms, 2004), dado que muitos dos métodos são idênticos por seguirem normas ou regras internacionais como a ISO27000, por exemplo. (Gillet et al., 2010). Hora & Klassen (2013) acrescentam que a aprendizagem pode ser feita através das práticas seguidas por outras organizações, tenham estas efeitos positivos ou negativos.

2.3.3.3. Corporativo

A Segurança de Informação, como já foi referido, não é exclusiva da área Informática ou Técnica. De facto, será necessário envolver toda a organização neste processo, uma vez que a simples aquisição de software, sem o envolvimento dos colaboradores para boas práticas, não é o suficiente para garantir uma maior segurança (Ellwanger et al., 2012).

A responsabilidade da Segurança da Informação é dos gestores seniores (Thomson & von Solms, 2005), sendo que o Quadro de Diretores deve ser também envolvido nesta gestão e agirem como referência para os outros colegas (van Osten, 2014). Contudo, deve ser parte da cultura corporativa (Astakhova, 2014) consciencializar todo o pessoal sobre estas políticas, através da consciencialização e do treino pessoal, bem como comunicar a intenção (como e porquê) da companhia em proteger os seus ativos e atribuição de penas para as pessoas que comprometam a segurança.

O papel que cada colaborador terá dentro da organização será diferente, consoante a sua função:

Executivos: Frameworks para uma visão geral da proteção dos dados

Gestores: Livros de regras para supervisionar e tomar decisões certas

Empregados: Visão clara do que lhes é esperado

A combinação destes três prismas deve ser utilizada dentro das organizações para maximizarem a sua Segurança. No entanto, apesar do conjunto de regras, tecnologia e processos minimizarem os riscos e os impactos em caso de ataque, não existe nenhum sistema que seja 100% seguro (Dutta & McCrohan, 2002).

2.4. PALAVRAS-CHAVE

Para a proteção da informação de uma organização, é necessário assegurar que sejam estabelecidas políticas e diversos procedimentos que protejam contra a sua modificação ou revelação não autorizada (Melro et al., 2007). Para tal é necessário definir um controlo de acessos que permita aos indivíduos acederem à informação a que têm direito (Sandhu & Samarati, 1996).

Esses controlos de acesso podem ser denominados como "Gestão de Identidade", em que se utilizam técnicas e procedimentos para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso (Melro et al., 2007).

Desta forma, uma das maneiras mais populares de proteger a informação é a autenticação através da combinação de nome de utilizador e palavra-chave (Pogue, 2011), em que será necessário identificar um indivíduo e colocar o respetivo código ou sequência de caracteres para aceder à informação pretendida. Este método é popular, pois têm um custo baixo comparativamente com outros métodos e são convenientes, ou seja, de fácil utilização (Yongzhong & Zhen, 2009), uma vez que basta ao indivíduo saber qual o seu nome de utilizador e respetiva palavra-chave (Sandhu & Samarati, 1996). Os métodos alternativos, segundo o mesmo autor, são algo que o utilizador tem, como um token ou smart card, ou ainda algo que o utilizador é, como os registos biométricos (retina ou impressões digitais).

A facilidade e a expansão da utilização de palavras-passe também tem o seu reverso. Segundo a Verizon (2013), quatro em cada cinco falhas reportadas foram sobre roubo de credenciais de autenticação. Como afirmam Naik & Sanyal (2012), quanto mais fácil for uma palavra-passe, mais fácil será para alguém adivinhá-la. Acrescenta-se que existem dois fatores que dificultam aos utilizadores a utilização de senhas de autenticação. O primeiro prende-se com a grande quantidade de serviços usufruídos pelas pessoas que utilizam palavras-chave. Em média, utilizam-se sete palavras-passe diferentes para 25 serviços diferentes (Acar et al., 2013), o que significa que se alguém descobre uma senha, pode entrar em diversos serviços (Ives et al.,

2004). O segundo problema prende-se com a memorização destas credenciais. Segundo Pilar et al. (2012), 72% das pessoas têm dificuldade em relembrar palavras-chave. Por um lado, a grande quantidade de regras para gerar uma senha de acesso leva a que os utilizadores cometam erros, como escrever as mesmas num papel e deixá-las perto dos computadores ("Ending the age of the password," 2005). Por outro as pessoas tentam que as suas palavras-chave tenham algo familiar para elas, enfraquecendo a segurança para ataques como os de dicionário (Brown et al., 2004).

As credenciais de autenticação não só servem para identificar um indivíduo, mas também para proteção de dados, sistemas e redes. O acesso aos Sistemas Operativos e aplicações tais como correio eletrónico, acessos remotos, proteção de ficheiros e outras informações (Scarfone & Souppaya, 2009).

Segundo Yongzhong & Zhen (2009), as palavras-chave devem estar disponíveis em computadores e serviços, sempre que solicitadas; o legítimo utilizador deve sempre efetuar o login na sua conta e estas devem ser user-friendly[7], ou seja, não causar transtornos aos utilizadores. Por fim, o custo de utilizar e implementar as credenciais de acesso deve ser reduzido e o serviço não deve perder qualidade caso a quantidade de novos utilizadores aumente.

2.5. GESTÃO DE PALAVRAS-CHAVE

Devido à grande popularidade das senhas de acesso (Pogue, 2011), uma boa gestão das palavras-passe é importante para prevenir problemas e perigos que advenham do seu roubo (Erdem et al., 2010), pelo que deve ser pertencer à política de segurança das organizações (Hitachi, 2014). Nesta parte serão descritos os riscos existentes à utilização das palavras-chave, tal como formas de mitigar os mesmos.

2.5.1. Riscos

Tal como Naik & Sanyal (2012) dizem, grande parte das autenticações utilizadas no mundo é através das palavras-passe. Existem uma série de ataques que os piratas informáticos podem proceder para tentarem aceder aos sistemas através das credenciais de acesso que serão seguidamente descritas, conforme o tipo que lhes pertence.

[7] Amigável para o utilizador. Significa que não deve causar problemas ao utilizador e a sua interface ser simples e clara

2.5.1.1. Adivinhação

Os ataques deste género visam acertar as senhas de acesso que um certo sistema tem, através de um de três métodos. Um é o ataque de força bruta, em que o hacker coloca uma série de combinações de diferentes caracteres e tamanhos de palavras-passe. Outro ataque parecido é um ataque de dicionário, em que o pirata informático coloca palavras conhecidas (de dicionário) para entrar numa conta de utilizador. O último ataque é um ataque híbrido, em que são utilizadas uma mistura dos dois ataques descritos anteriormente, ou seja, junta-se palavras de dicionário com números e símbolos e algumas combinações comuns, como por exemplo "1" por "I". Este último é mais abrangente que o ataque de dicionário e mais rápido que os ataques de força bruta.

2.5.1.2. Engenharia social

São ataques em que o hacker tenta aproveitar-se das condições à volta do utilizador e dos informáticos do sistema para entrar no mesmo. Um ataque é o *shoulder surfing*, em que o pirata informático encontra-se perto do utilizador e vê qual a palavra-chave introduzida. O outro ataque é feito através da recuperação e *reset* à senha de acesso. O hacker faz-se passar por um utilizador e pede à equipa de informática para lhe fazerem *reset* à palavra-passe, por exemplo, via telefone. Na volta, a informática informa-o da nova credencial de autenticação.

2.5.1.3. Servidores e outros ataques

Estes ataques são feitos aos servidores onde estão alojadas as informações dos utilizadores ou necessitam de outros métodos para que as palavras-chave sejam descobertas. *Cracking* é o método em que o hacker tenta descobrir qual a senha criptográfica, através de várias análises, para entrar no sistema. Ataque de pote de mel é um ataque direto aos servidores onde as palavras-chave estão alojadas, para recolha das mesmas ou para atacar outros servidores. Outro modo é apanhar as senhas de acesso quando estas estão a circular na rede, enquanto os utilizadores autenticam-se. Esta variante é conhecida como transmissão. Um último ataque é o *keylogger*, em que o hacker coloca um malware (por exemplo, Cavalos de Troia) ou um dispositivo físico (em terminais públicos), em que é enviado ao pirata informático as teclas pressionadas por um utilizador, transmitindo os dados de autenticação.

2.5.2. Mitigação

Como o artigo "Ending the age of the password" (2005) refere, o utilizador final é o elo mais fraco, pois é o próprio que tem de gerir e escolher as suas palavras-chave, como as decide memorizar ou gravar e, em último caso, é o próprio que corre riscos para a sua segurança virtual, ao clicar em links suspeitos de emails, fazer o download de programas gratuitos, entre outros.

As melhores práticas recomendadas por outras organizações, como Scarfone & Souppaya (2009), Cantwell (2010), SANS Institute (2014) ou Hitachi (2014) sugerem, como o tamanho mínimo das senhas, a obrigatoriedade de se utilizar diferentes tipos de caracteres, palavras-chave com data de expiração e a proibição de se repetirem são dos métodos de mitigação mais comuns. Conforme a Tabela 4 mostra, através de um estudo do Splashdata, os utilizadores continuam a escolher palavras-passe facílimas de lembrar em serviços que não têm regras específicas para criarem as mesmas, sendo que as mais fáceis de detetar e quebrar são "123456", "password" e "12345678".

Ranking	Palavra-chave	Posição relativa a 2012
1	123456	+ 1
2	Password	- 1
3	12345678	-
4	Qwerty	+ 1
5	abc123	- 1
6	123456789	Novo registo
7	111111	+ 2
8	1234567	+ 5
9	Iloveyou	+ 2
10	adobe123	Novo registo

Tabela 4 – Piores palavras-chave de 2013
Fonte: splashdata (2014)

Uma das recomendações sugeridas para aumentar a proteção das senhas de acesso passa por revelar aos empregados a importância da Segurança da Informação, uma vez que grande parte dos riscos partem de acções negligentes por parte dos próprios (Thomson & von Solms, 2005). Assim, a divulgação de sugestões para não

utilizar dados pessoais ou familiares ao criar as palavras-passe, ou não repetir as mesmas senhas de acesso para sistemas diferentes seriam mais absorvidas e utilizadas no dia-a-dia da empresa, uma vez que são recomendações, dado que o sistema não consegue "ler" as palavras que compõe as palavras-chave. Por exemplo, "Password1" cumpre as regras da companhia (tem mais de 8 caracteres e cumpre 3 dos 4 requisitos – letras em maiúsculas, letras em minúsculas e um número) e, no entanto, é das palavras-passe mais fracas que existe na atualidade (Campbell et al., 2007).

Uma outra sugestão seria tornar as palavras-passe mais difíceis de adivinhar, através de regras mais apertadas. Vários exemplos são dados em Pogue (2011), em que junta dois exemplos. Num, as pessoas são obrigadas a terem um mínimo de 8 caracteres nas suas senhas, devem cumprir os 4 requisitos (maiúsculas, minúsculas, números e caracteres especiais) e a mesma muda a cada 30 dias. No outro, as credenciais de acesso têm de ter 12 caracteres, são alfanuméricas, mas fornecidas por um indivíduo da área informática. Também mudam a cada 30 dias. No entanto, uma maior quantidade de obrigatoriedades não corresponde a palavras-passe mais seguras (Campbell et al., 2007). Tal como Pilar et al. (2012) afirmam, quanto mais as credenciais de autenticação forem difíceis de adivinhar, mais difícil é aos utilizadores lembrarem-se das mesmas, pelo que utilizam caraterísticas fáceis de identificar: palavras com significados especiais, palavras-passe o mais curtas possíveis, apontam as mesmas em papéis ou noutros suportes ou reutilizam as palavras-chave para sistemas diferentes.

Contudo, existe quem defenda que as regras acima mencionadas não sejam as melhores que se possam aplicar, uma vez que faz com que os utilizadores tenham muitas palavras-chave, com regras mais ou menos similares, levando a que os mesmos criem senhas de acesso fracas, como "Password1" (Cantwell, 2010). Assim, Singer & Anderson (2013) defendem que uma organização deve ter apenas uma palavra-passe para todos os sistemas da mesma (conhecido como single sign-on). A senha seria gerada de modo aleatório, para evitar que os colaboradores criem palavras-chave fracas. Um colaborador que utilize um computador pode ter uma credencial mais curta, mas que utilize letras (maiúsculas e minúsculas), símbolos e números, ao passo que os utilizadores de *tablets* e *smartphones* podem preferir as passphrase[8], que são mais longas, mas mais fáceis de digitar nos teclados destas máquinas. A palavra-passe poderia ser anotada, contanto que seja feito de um modo seguro. Esta palavra-chave

[8] Sequência de letras ou outro texto para controlo de acesso a um sistema. Geralmente são mais longas que as palavras-chave

não seria mudada com frequência, apenas quando se se verificasse ou suspeitasse de que a mesma poderá ter sido comprometida. Por fim, aconselham a que os utilizadores não utilizem esta palavra-passe nos sistemas fora da companhia. Sobre este assunto, Tiwari & Joshi (2009) acrescentam que o método de single sign-on simplifica a administração de IT, pois para cada utilizador existe apenas uma senha de autenticação, requer poucas mudanças na infraestrutura da empresa para implementar este género de autenticação e aumentaria a produtividade, uma vez que os utilizadores apenas teriam de se recordar de uma palavra-passe, que serve para múltiplos sistemas.

Por fim, existem outros modos de proteger as palavras-chave. Jacobs (2011) argumenta que, com a quantidade de senhas que as pessoas utilizam, os utilizadores podem precisar de registar as mesmas numa lista, mas que deve ser protegida num local seguro. Como exemplo, dá um gestor de palavras-passe virtual, embora basta descobrir uma credencial de autenticação para entrar em todos os serviços desse utilizador; um documento encriptado, mas que sofre um problema similar ao do gestor de palavras-chave virtual; armazenar na nuvem o documento encriptado, pese que basta algum pirata informático aceder ao link e desencriptar o documento; uma pen USB, que deverá ser mantida em local seguro.

Um outro método sugerido é a utilização de dois tipos de autenticação nos sistemas, mas que seria igualmente simples de se utilizar. Como Erdem et al. (2010) apresentam, um smart card seria uma solução em que no cartão seriam armazenadas as palavras-passe, com o máximo de proteção possível e o acesso aos sistemas seria praticamente automático. O utilizador apenas teria que ligar o smart card ao computador e inserir um PIN. Deste modo, o utilizador teria que ter posse de algo (o smart card) e teria de saber um código (PIN), ou seja, um sistema com dois fatores de autenticação, mas que tem a conveniência do single sign-on.

3. METODOLOGIA

Para a realização deste trabalho, várias metodologias foram realizadas, de acordo com as necessidades de cada objetivo.

No cômpito geral, foi escolhido um caso de estudo, dado que o grande objetivo é descrever ou analisar o fenómeno da gestão de palavras-passe de forma profunda e global (Yin, 2009). Tal como o autor refere, um caso de estudo investiga um fenómeno contemporâneo, pretendendo explicar o mesmo. Neste caso, observar-se-á a gestão das palavras-chave num ambiente natural, sendo que os dados serão daí retirados (Santos, 2013).

Para a compreensão da complexidade do risco operacional e dos processos de gestão de palavras-chave, foi feita uma revisão da literatura, de modo a conhecer a visão que alguns autores têm sobre este tema e a sua importância para a sociedade atual.

Por outro lado, a descrição do processo de gestão de credenciais de autenticação da seguradora em questão e a identificação dos pontos de controlo tiveram como base a documentação existente na organização e a experiência própria na criação de palavras-passe e esclarecimento de dúvidas.

A identificação dos riscos existentes teve como base dois processos diferentes. Num, foi utilizada a literatura existente de autores e organizações conceituadas que indicam os riscos que estes processos de gestão têm de enfrentar. No outro processo, foi efectuado um questionário eletrónico, via Internet (link para um site) a todos os colaboradores da organização, dado que todos têm um computador com acesso à Internet, não havendo restrições geográficas. Pode ser respondido no momento da conveniência do utilizador, para além de ser de fácil e rápida utilização. O custo deste género de inquérito é nulo, sendo que foi utilizado o Google Form para elaboração do mesmo. As respostas serão maioritariamente fechadas e semiabertas (lista fechada de respostas mais uma aberta), para evitar a heterogeneidade de respostas (Vilares & Simões Coelho, 2011). As respostas permitiram verificar, por um lado, os erros que se pode estar a cometer na gestão das palavras-passe, e por outro, verificar qual a importância que dão à gestão e criação de palavras-passe, e consequentemente, a sua opinião no que respeita à segurança da informação. Uma das limitações encontradas no inquérito realizado foi a idade dos colaboradores ser escrita e não estar inserida num intervalo que permitisse aos inquiridos “esconder” a sua identidade ou evitar respostas “fora do limite”, como por exemplo, indicar que se tem 100 anos de idade.

Outra limitação do inquérito foi o facto de algumas das respostas ao mesmo estarem erradas, como no exemplo em que, ao perguntar o motivo de repetir palavras-passe em sistemas diferentes, a resposta tenha sido que não repetiam as senhas. O inquérito realizado, bem como os seus resultados, encontram-se disponibilizados em anexo.

No último passo, sobre a mitigação do risco, será baseada também na literatura existente sobre o tema, tanto de autores individuais, como de organizações especializadas e boas práticas que outras empresas podem ter. As recomendações e sugestões de melhoria que estes artigos apresentarem serão comparados com os processos atuais da companhia em estudo, de modo a retirar e analisar aqueles que poderão acrescentar valor à gestão segura e eficaz das palavras-passe da organização.

4. RESULTADOS E DISCUSSÃO

4.1. ANÁLISE AO PROCESSO DE PALAVRAS-CHAVE NA SEGURADORA

Neste ponto, serão descritas como a empresa gere as palavras-passe dos seus colaboradores, nomeadamente quando estes entram na organização ou quando pedem um *reset* às suas palavras-chave, quando não se lembram das mesmas. Outro ponto será a descrição de como a seguradora em estudo protege as suas senhas de acesso contra as ameaças.

4.1.1. Descrição do processo

Para a criação de uma primeira palavra-chave, os Recursos Humanos recolhem o nº de Contribuinte (ou o nº do passaporte, caso o colaborador seja estrangeiro) e registam esse número numa Base de Dados, ligado ao número de colaborador respetivo. Caso o colaborador seja externo, o *manager* registará o NIF numa aplicação dos Recursos Humanos, juntamente com os outros dados pessoais.

A Base de Dados fará com que apenas os últimos quatro dígitos do número de contribuinte estejam disponíveis para a equipa responsável na área informática para a criação e gestão dos acessos informáticos, de modo a que a primeira palavra-passe de acesso ao sistema sempre que um colaborador entre seja genérica para todos que entrem na companhia e simultaneamente desconhecida para outras pessoas que eventualmente vejam a mensagem.

A primeira palavra-passe de acesso ao sistema é algo como “Seguradora1234”, em que “1234” representam os quatro últimos dígitos do número de contribuinte, que será indicada à chefia direta ou diretamente ao novo colaborador, referindo que a mesma é “Seguradora” seguida dos últimos quatro dígitos do NIF.
Para efectuar o *reset* à senha de acesso ao Windows, o colaborador indica à equipa informática que precisa de um *reset* à palavra-chave, sendo que a senha reposta será indicada ao colaborador como “Seguradora” seguida dos últimos quatro números do cartão de contribuinte. Este processo encontra-se esquematizado na figura 3.

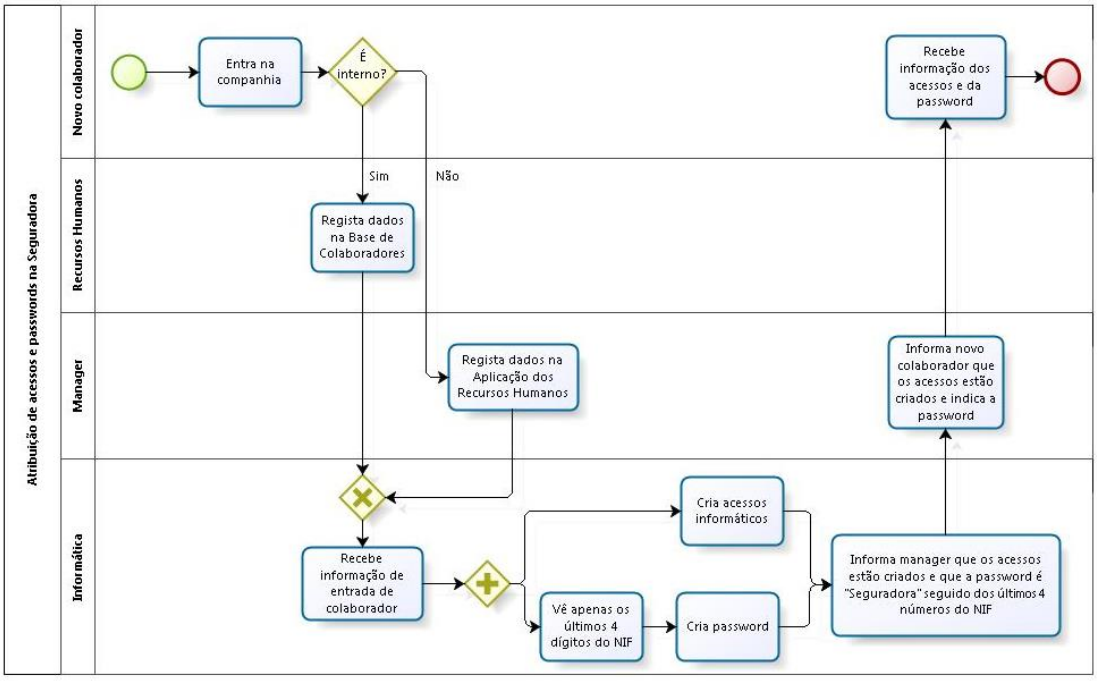


Figura 3 – Atribuição de acessos e palavras-chave na Seguradora

Fonte: Elaboração própria

4.1.2. Pontos de controlo

De modo a mitigar possíveis riscos inerentes à gestão e utilização de palavras-chave, a companhia tem um conjunto de regras que estão escritas na sua regulamentação interna.

As credenciais utilizadas devem ter um mínimo de 8 caracteres e seguir pelo menos três das quatro regras de caracteres: letras em minúsculas, letras em maiúsculas, numeração árabe ou caracteres não alfanuméricos (sinais de pontuação). Estes são recomendados tanto por Hitachi (2014), como por Naik & Sanyal (2012). Tal como Rowan (2009) indica, e vendo pela Tabela 5, quanto mais forem os caracteres utilizados, em termos de quantidade, combinados com uma palavra-passe maior, maior é a complexidade da mesma. Por exemplo, uma palavra-chave de 4 caracteres em que estes sejam apenas números (10), permite algo como 546 senhas de acesso possíveis. Em comparação com credenciais de autenticação alfabéticas (26) com um tamanho de 4 caracteres, permite 7421 combinações de palavras-passe. Brown et al. (2004) recomenda ainda que os caracteres especiais devem ser utilizados no meio da senha de acesso, de modo a dificultar os ataques de dicionário mistos com números e símbolos especiais no fim da palavra-chave.

Tamanho do conjunto	Tipo de caracteres				Tamanho Palavra-chave				
	Dígitos	Letras	Símbolos	Outros	4	8	12	16	20
10	Decimal				1*10^4	1*10^8	1*10^12	1*10^16	1*10^20
16	Hexadecimal				7*10^4	4*10^9	3*10^14	2*10^19	1*10^24
26		Tamanho insensitivo			5*10^5	2*10^11	1*10^17	4*10^22	1*10^28
36	Decimal	Tamanho insensitivo			2*10^5	3*10^12	5*10^18	8*10^24	1*10^31
46	Decimal	Tamanho insensitivo	10 Comuns[9]		4*10^6	2*10^13	9*10^19	4*10^26	1*10^33
52		Maiúsculas e minúsculas			7*10^6	5*10^13	4*10^20	3*10^27	1*10^34
62	Decimal	Maiúsculas e minúsculas			1*10^7	2*10^14	3^10^21	5*10^28	1*10^35
72	Decimal	Maiúsculas e minúsculas	10 Comuns		3*10^7	7*10^14	2*10^22	5*10^29	1*10^37
95	Decimal	Maiúsculas e minúsculas	Todos os símbolos em teclados standards		3*10^7	7*10^15	5*10^23	4*10^31	1*10^39
222	Decimal	Maiúsculas e minúsculas	Todos os símbolos em teclados standards	Todos os outros caracteres ASCII	2*10^9	6*10^18	1*10^28	3*10^37	1*10^46

Tabela 5 – Possíveis tamanhos de palavras-chave por comprimento da senha e tamanho dos conjuntos de caracteres
Fonte: Scarfone & Souppaya (2009)

O sistema da companhia obriga a que, pelo menos de 90 em 90 dias a credencial de autenticação seja modificada, tal como a maioria das organizações obriga (Jacobs, 2011), embora o processo seja ineficaz se o hacker conhecer a senha antiga e descobrir a nova pelo mesmo método, como por exemplo, com um keylogger[10] (Scarfone & Souppaya, 2009). Um utilizador só pode mudar a palavra-chave uma vez por dia.

A idade mínima de palavras-passe é o tempo necessário que o utilizador tem de esperar até voltar a trocar a palavra-chave. Este caso está relacionado com o histórico das senhas de autenticação, que impede um utilizador de repetir a mesma credencial de acesso durante X palavras-passe. Estas combinações impedem que as senhas sejam mudadas as vezes suficientes num curto espaço de tempo até o utilizador conseguir voltar a utilizar a mesma (Scarfone & Souppaya, 2009). No caso desta seguradora é um dia para voltar a mudar a senha e 12 palavras-chave guardadas em histórico. No caso desta reutilização da palavra-passe no mesmo sistema não é grave, uma vez que

[9] Considerados os símbolos que aparecem nas teclas de 0 a 9: !@#$%^&*()

[10] Programa de computador que regista tudo o que é digitado, para capturar, entre outros, palavras-chave ou números de cartões de crédito

apenas 9% das respostas indicam que reutilizam as mesmas senhas ao fim de 12 palavras-passe diferentes.

Para proteção contra ataques diretos de hackers, o sistema bloqueia automaticamente ao fim da 3ª tentativa errada seguida de acesso. Este é um dos métodos de bloqueio contra ataques que Yongzhong & Zhen (2009) identificam, juntamente com o atraso na resposta se a tentativa de acesso for errada, o que diminui a quantidade de ataques. O contra destes dois métodos é que o utilizador, no primeiro caso fica também bloqueado quando quiser entrar, no segundo pode demorar a conseguir aceder ao sistema. Para reativar a palavra-passe, o utilizador primeiramente deverá responder a duas de cinco questões de controlo que previamente escolheu, como recomenda Solove (2003), pois o hacker terá que conhecer e recolher muita informação pessoal do colaborador para conseguir ultrapassar este obstáculo.

Quando a informática cria ou faz um *reset* uma palavra-passe, esta é feita em modo expirado, para obrigar o utilizador a mudar a palavra-chave na primeira vez que entra no sistema.

Na companhia, existem algumas recomendações que devem ser seguidas pelos colaboradores. As palavras-chave não devem conter palavras que sejam encontradas num dicionário, nem conter o nome completo do utilizador, nem o nome de utilizador (conhecido como userID ou username), nem o nome da companhia e também evitar reutilizar ou "reciclar" palavras-passe antigas.

Não se deve incluir palavras-chave em sistemas automatizados de *logon*, como macros ou teclas de função. As credenciais de acesso são confidenciais e não devem ser reveladas a terceiros em nenhuma circunstância, sob pena de sanções graves.

Sempre que se suspeite ou detete que a confidencialidade da palavra-passe foi comprometida, o utilizador deve alterar a palavra-chave e a equipa de informática deve ser contactada sempre que se suspeitar que o sigilo da senha foi comprometido.

4.2. RESPOSTAS AO INQUÉRITO

No inquérito enviado a toda a organização, 43% dos colaboradores responderam ao mesmo, verificando-se que entre homens e mulheres a diferença no número de repostas não é grande (cerca de 8%). Por idade, o grande bolo de respostas equivale às faixas etárias correspondidas entre os 30 e 50 anos, incluindo uma resposta inválida,

neste campo. No extremo oposto, estão as pessoas com menos de 30 anos, com 14% de respostas ao inquérito.

Em termos de tempo de casa, as pessoas com 4 a 20 anos de casa foram as que responderam mais ao inquérito, contrastando com as pessoas que estão há pouco tempo na companhia. Obviamente que existe esta discrepância, pois o número de pessoas com menos tempo de casa (um ano, neste caso) é substancialmente menor às que já estão há mais tempo, salvo se a empresa fosse relativamente recente.

Relativamente ao departamento em que trabalham, praticamente metade das respostas foram dadas por pessoas da área comercial, o que não surpreende, pois numa empresa de seguros, espalhada por todo o país, esta área é substancial para o negócio. Os outros departamentos com mais respostas foram o de sinistros, seguido da técnica e atuariado e o financeiro e planeamento. O departamento institucional foi o que menos respostas obteve, dado que é um dos menores departamentos da organização. O "vários" representa todos os departamentos que não tiveram representação própria no inquérito, sendo estes a administração (CEO), auditoria, jurídico, marketing, secretariado, recursos humanos e pessoas que trabalham a nível internacional, pois são demasiado pequenos para que as respostas dos colaboradores mantivessem a sua confidencialidade.

Por fim, verifica-se que a maioria dos colaboradores utiliza mais de três palavras-chave na companhia (42%). No extremo oposto, apenas 23 pessoas responderam que utilizam apenas uma credencial de autenticação para desempenharem o seu trabalho. Neste aspeto, convém ter em atenção que uma palavra-passe permite o acesso a diversos sistemas, sendo inclusive um dos motivos para que as respostas à questão "Porque utiliza as mesmas passwords para sistemas diferentes" ter uma resposta como a obrigatoriedade dos sistemas utilizarem a mesma palavra-chave.

Ainda no contexto global, verifica-se que cerca de 57% das respostas indicam que as pessoas utilizam as mesmas senhas de acesso para aceder a sistemas diferentes, com a agravante de alguns sistemas utilizarem a mesma palavra-chave para acesso, conforme descrito no parágrafo anterior. Ainda assim, equivale a mais 14% em relação aos que não repetem as palavras-passe. Entre as respostas mais dadas sobre o motivo de repetirem as palavras-chave, verifica-se que 89% indica que é por ser mais fácil de memorizar. Por outro lado, das pessoas que não repetem as senhas de autenticação, 59% diz que é por se preocuparem com a segurança da informação. Por último, 36% dos colaboradores aponta as credenciais de acesso para não se

esquecerem das mesmas. Destes, alguns tomam cuidados especiais para que as suas palavras-chave não caiam em mãos erradas, como verificado na tabela 6. A maioria escreve as suas senhas de autenticação codificadas, de modo a que, se alguém ler os apontamentos, não descobrir diretamente as palavras-passe. Outros colaboradores anotam as palavras-chave em softwares especiais de gestão de senhas, em que basta conhecer um código para aceder às palavras-chaves. Entre outros cuidados, algumas pessoas apontam em blocos de notas ou agendas que andam sempre com as mesmas, o que, em caso de roubo dos apontamentos, não impede a descoberta dos códigos. Alguns colaboradores ainda colocam as palavras-passe em locais de difícil acesso ou numa gaveta trancada por eles próprios.

Agenda/bloco com as próprias pessoas	4
Gaveta trancada	1
Código em local de acesso difícil	2
Codificação	28
Software com código	7

Tabela 6 – Proteção das palavras-chave escritas na Seguradora
Fonte: Elaboração própria

Nas questões relacionadas com a partilha de palavras-passe, verifica-se que a 4 colaboradores já lhes foi solicitado para que partilhasse as suas credenciais de autenticação. Destes, verifica-se que metade já chegou a partilhar senhas de acesso, embora não se saiba se foi em consequência destes pedidos. Verifica-se que a três destes colaboradores foi-lhes pedido mais que duas vezes para partilhar as palavras-chave.

No entanto, 21 pessoas que responderam ao inquérito indicaram que já partilharam senhas de autenticação com colegas, das quais 10 já o fizeram mais que duas vezes. Segundo as próprias, apenas foi para um sistema que partilharam as suas palavras-chave. Dos motivos indicados para a partilha (ver tabela 7), 13 pessoas dizem que foi por falta de acessos atribuídos (três reclamaram urgência no pedido), cinco por ausência e duas indicaram que foi a pedido da área informática. Uma pessoa diz que foi por ter problemas no telemóvel. Das vinte e uma pessoas que partilharam a sua palavra-chave, 17 mudaram a sua senha de autenticação após a utilização por parte do outro colega.

Porque motivo partilhou passwords?	
Falta de acessos	13 (3 reclamam urgência)
Ausência	5
Informática (a pedido de)	2
Telemóvel	1

Tabela 7 – Motivos de partilha de palavras-chave na Seguradora
Fonte: Elaboração própria

Numa questão sobre a partilha das senhas de autenticação, ou seja, como consideram o ato de partilhar credenciais de autenticação numa escala de 1 a 5, em que 1 não representa gravidade a 5 que representa muito grave, cinco colaboradores acham que não existe gravidade em partilhar palavras-passe, ao passo que 66% considera que partilhar palavras-chave é algo muito grave. As restantes respostas centram-se mais no nível 4 (24%). Curiosamente, das cinco pessoas que não acham que partilhar senhas de acesso seja grave, nenhuma indicou que até agora tenha partilhado as mesmas.

Na outra questão opinativa, em que se perguntou se o inquirido partilhasse uma credencial de acesso a um colega e este fizesse algo grave, de quem seria a culpa, três pessoas indicaram que seria o colega, pois foi ele que trabalhou no sistema. Uma dessas pessoas já partilhou a sua palavra-passe com colegas. A grande maioria das pessoas (65%) indicou que o ónus seria da própria, pois foi ela que partilhou a palavra-chave ao colega. As restantes respostas foram direcionadas para a culpa própria, pois foi o próprio nome de utilizador que fica registado no sistema. A resposta "Dele, pois tenho um email a indicar que lhe partilhei a password" não obteve nenhuma resposta.

Nas questões específicas para o sistema Windows, 95% indicou que apenas muda a senha de acesso quando o sistema obriga a tal, enquanto que das restantes respostas, 10 pessoas indicam que alteram à sua medida, mesmo antes do sistema avisar que tem de alterar a credencial de autenticação. As restantes quatro pessoas alteram quando o sistema avisa que têm alguns dias para mudar a palavra-chave.

Quando os colaboradores têm de mudar a sua senha, 171 colaboradores (56%) muda apenas um carácter da sua palavra-passe, o que perfaz uma diferença pequena em relação aos outros colegas (ou seja, 37 pessoas), que alteram mais radicalmente as suas palavras-chave.

Em relação à constituição das credenciais de autenticação, 218 indivíduos disseram que não utiliza palavras conhecidas para a criação das mesmas, dentro do possível. Das restantes pessoas, como se pode ver pela tabela 8, trinta e nove utilizam

nomes de familiares como referência para as suas senhas de acesso. Verifica-se que, das 19 pessoas que indicaram fazer referência a nomes de familiares, utilizam também outras palavras para formar as suas palavras-chave. Entre os requisitos para cumprir as palavras-passe no Windows, 195 colaboradores utilizam o mínimo exigido (3), ao passo que o restante pessoal cumpre os 4 critérios recomendados.

Utiliza que género de palavras para criar as suas passwords?	
Nomes	39
Datas	18
Animais	8
Títulos	8
Nomes de familiares e outras referências	19
Outras referências (não especificado)	19

Tabela 8 – Referências para criação de palavras-chave na Seguradora
Fonte: Elaboração própria

Por fim, verifica-se que, ao fim da utilização de 12 palavras-chave para entrar no sistema operativo, 160 pessoas disseram que não volta a utilizar as mesmas senhas, ao passo que 38% das respostas indicam que não se lembram ou esta pergunta não se aplica à sua situação.

4.2.1. Análise por idades

Verifica-se que os colaboradores a partir dos 30 anos têm, na sua maioria, mais de 3 palavras-chave na companhia para desempenhar o seu trabalho. Os jovens com menos de 30 anos têm três senhas de acesso associadas.

A percentagem de utilizadores que utilizam a mesma credencial de autenticação para sistemas diferentes, sempre que tal é possível, é maior nos mais jovens e tem uma ligeira quebra, conforme o aumento da idade. Em sentido oposto, quanto mais jovem for o escalão etário, menor é a percentagem que anota as palavras-chave para não se esquecerem das mesmas.

Em relação à partilha das senhas, às pessoas nas faixas etárias entre os 20 e os 30 anos e os 50 a 60 anos, nunca lhes foi solicitado que partilhassem as suas palavras-passe, embora já tenham partilhado credenciais de acesso com colegas, não havendo, em termos de probabilidades, nenhuma faixa etária que se tenha destacado. Em todos os escalões, existiram pessoas que, depois de partilharem as palavras-chave, mudaram

e mantiveram as suas senhas, exceto para o escalão maior que 50 anos, uma vez que as duas pessoas que responderam que partilharam palavras-passe alteraram a sua senha de autenticação.

Quando se questiona sobre a opinião em relação à partilha das palavras-chave, verifica-se que o escalão mais jovem apresenta respostas a partir do nível 3, ao passo que nas outras faixas existiram respostas que indicavam que não viam nenhuma gravidade no ato de partilhar senhas de acesso. Contudo, por outro lado, a percentagem de respostas de pessoas que consideram muito grave esta questão é sempre maior que 50%, aumentado consoante o escalão mais velho.

Sobre o Windows, verifica-se que o escalão mais jovem apenas muda a palavra-passe quando o sistema o obriga a tal, sendo que esta percentagem vai diminuindo ao longo do tempo. Verifica-se um ligeiro aumento percentual, do escalão mais novo ao mais velho, no número de respostas afirmativas se muda apenas um carácter quando muda de senha de acesso. Em relação à composição das palavras-chave, os escalões intermédios (entre os 30 e 49 anos) são aqueles que mais utilizam palavras conhecidas para as mesmas e são os que cumprem o mínimo de 3 requisitos.

4.2.2. Análise por tempo de casa

Os colaboradores com menos tempo de casa (menos de um ano) são os que têm menor número de senhas de autenticação na companhia.

Verifica-se que não existem grandes diferenças nas respostas se utilizam as mesmas palavras-chave para sistemas diferentes, sendo que as respostas positivas são ligeiramente superiores que as negativas. Quanto maior for o tempo de casa, maior é a percentagem de pessoas que anotam as suas senhas de acesso para não se esquecerem. Neste caso, poderá estar relacionado com a idade, uma vez que uma pessoa com mais de 20 anos de casa terá mais anos de vida que uma que trabalhe há menos tempo.

Tal como no registo das idades, aos extremos (menos de um ano e mais de 20 anos de casa) nunca lhes foi pedido que partilhassem palavras-passe. Contudo, apenas as pessoas que estão há menos tempo na companhia nunca partilharam senhas de acesso. Das que partilharam, todas as que têm pelo menos 10 anos de casa alteraram as suas palavras-chave após a partilha.

Quando se pergunta de quem será o ónus se o colaborador partilhar uma credencial de autenticação, a grande maioria das respostas indicou que seria dos

próprios, pois seriam eles que partilharam a palavra-passe. Ninguém nas faixas 1 a 3 anos, 10 a 20 anos e mais de 20 anos deram a primeira resposta (que a culpa seria do colega, pois seria ele que trabalhou no sistema).

Todos os que trabalham na companhia há menos de um ano apenas mudam a palavra-chave quando o sistema o obriga a tal. Para escolher as suas palavras-passe, as pessoas com 1 a 3 anos de casa são as que mais utilizam palavras conhecidas, contra os 22% das pessoas com mais de 20 anos de casa. Na escolha das senhas de acesso, os utilizadores com 1 a 3 anos de casa são também os que têm maior percentagem de cumprirem apenas os mínimos dos requisitos para as suas palavras-chave.

4.2.3. Análise por departamento

Verifica-se que o departamento informático é o que tem mais credenciais de autenticação na companhia, sendo que inclusivamente ninguém desse departamento deu a resposta mínima. Por outro lado, apenas uma pessoa do departamento financeiro e planeamento e do institucional disse que tem apenas uma senha de acesso na companhia. Sobre a repetição de palavras-chave, no departamento institucional todos disseram que utilizam as mesmas palavras-passe, mas convém lembrar que neste departamento apenas houve 6 respostas. Os departamentos onde o maior número de pessoas anota as suas senhas (com valores na casa dos 40%) são o comercial, o financeiro e planeamento e o de sinistros.

Os departamentos comercial, técnica e atuariado e informática foram aqueles onde foram pedidas às pessoas que partilhassem palavras-chave. Neste último departamento, a essas pessoas foi-lhes solicitado mais que uma vez a partilha de palavras-passe. O departamento onde se partilham mais palavras-chave, percentualmente falando, é o da técnica e atuariado, embora em valores absolutos seja o departamento comercial. Por outro lado, é novamente o departamento informático em que, quando partilham senhas de acesso, partilham mais de duas vezes, com 100% de respostas neste ponto. Após a partilha das palavras-chave, nos departamentos comercial e de sinistros existem pessoas que não mudaram a credencial de autenticação, bem como a pessoa que se encontra num departamento geral (“Diversos”).

Quando se pergunta se se partilhasse uma senha de acesso com um colega, de quem seria a culpa caso algo corresse mal, apenas as pessoas na direção financeira e planeamento e dos sinistros responderam que seria do colega, dado que foi ele que executou o trabalho. Nas restantes respostas não houve muitas diferenças.

Os departamentos financeiro e planeamento e institucional mudam as suas palavras-passe apenas quando o Windows obriga a tal. Por outro lado, o departamento com menor percentagem é o informático, mas apenas com 91%. As pessoas no departamento técnico e atuariado são as que mudam apenas um carácter quando alteram as suas senhas de acesso, com 73% de respostas nesta categoria. Os outros departamentos mantêm-se próximos dos 50%, salvo o institucional, com 33%.

O departamento que utiliza menos palavras conhecidas para gerar as suas palavras-passe é o informático, com 18% de respostas positivas. Excluindo o departamento institucional, todos os outros também têm respostas positivas abaixo dos 50%. Por outro lado, os departamentos com maiores taxas de resposta em que cumprem apenas os requisitos mínimos para compor as suas credenciais de acesso são o comercial e o financeiro e planeamento, na ordem dos 70%, aproximadamente.

4.2.4. Análise por número de palavras-chave

Verifica-se que a utilização das mesmas palavras-passe para sistemas diferentes tem valores percentuais semelhantes, não se detetando inclusive um aumento substancial nos utilizadores que utilizam mais de três palavras-chave dentro da companhia. Os utilizadores que indicaram que apenas usam uma senha de acesso no trabalho, mas utilizam credenciais de autenticação diferentes na companhia não foram contabilizados para estas respostas, uma vez que deverá ter-se tratado de confusões dos mesmos neste inquérito. Ao perguntar se anotam as suas senhas de acesso para não se esquecerem, existe um aumento substancial para as pessoas que utilizam mais de três palavras-chave. Das que indicaram que utilizam apenas uma, apenas uma anota essa palavra-passe para não se esquecer.

Relativamente à partilha de palavras-passe, apenas aos que têm apenas uma ou mais de três senhas é que lhes foi solicitado que partilhasse a mesma, sendo que aos que têm mais palavras-passe esta solicitação foi feita mais de 2 vezes. Em relação à partilha, todos os grupos já partilharam palavras-chave, não se registando diferenças substanciais entre os mesmos. Contudo, verifica-se que o agregado com mais credenciais de autenticação é aquele que indica que já partilhou senhas mais que duas vezes. Após a partilha, todos os grupos indicaram ambas as respostas se mudaram as suas palavras-passe, destacando-se o facto de, quanto maior o número de palavras-chave, maior é a percentagem de pessoas que muda as suas senhas de acesso.

Em relação à gravidade de partilha de credenciais de autenticação, verifica-se que, quanto maior o número de palavras-passe que os colegas têm, mais grave consideram a partilha de palavras-chave. Por outro lado, embora praticamente todas as respostas indiquem que, caso partilhem uma senha de acesso, o ónus será dos próprios, verifica-se que quem tem apenas uma palavra-passe para utilizar na companhia, diz que a culpa será do próprio, pois o sistema registaria o seu nome de utilizador e não o do colega.

Nas mudanças de senhas para o Windows, não existe grande diferença entre os grupos, sendo que praticamente todos indicam que mudam as suas palavras-chave apenas quando o sistema obriga. Contudo, nota-se um ligeiro decréscimo à medida que o número de palavras-passe aumenta. Na altura da mudança de senha de acesso, também não se registam grandes alterações entre os grupos, registando-se valores entre os 52% e 59% de pessoas que muda apenas um carácter.

Nas questões sobre a forma das credenciais de autenticação, verifica-se semelhanças entre as pessoas com uma e mais de três palavras-passe. São estes grupos, comparativamente aos outros dois que menos utilizam palavras conhecidas para gerar credenciais de autenticação e, simultaneamente, os que mais cumprem os 4 requisitos para a geração de senhas de acesso.

4.2.5. Análise por género

Nas diferenças por género, verifica-se que os homens com mais de três palavras-passe têm um maior valor percentual que as senhoras. Nas questões de utilizarem as mesmas palavras-chave para sistemas diferentes e apontarem as suas senhas de acesso não se encontram diferenças significativas entre os conjuntos.

Nas questões por partilha também não se registam diferenças, salvo que os homens partilham mais vezes as suas credenciais que as senhoras, num total de 54% contra 38% na opção "Mais que 2 vezes". Também é o género masculino que mais muda as palavras-chave após a partilha.

No ato de geração de senhas, as mulheres são as que mais utilizam palavras conhecidas para as mesmas (33% contra 25%) e são também quem cumprem os requisitos mínimos (67% contra 62%).

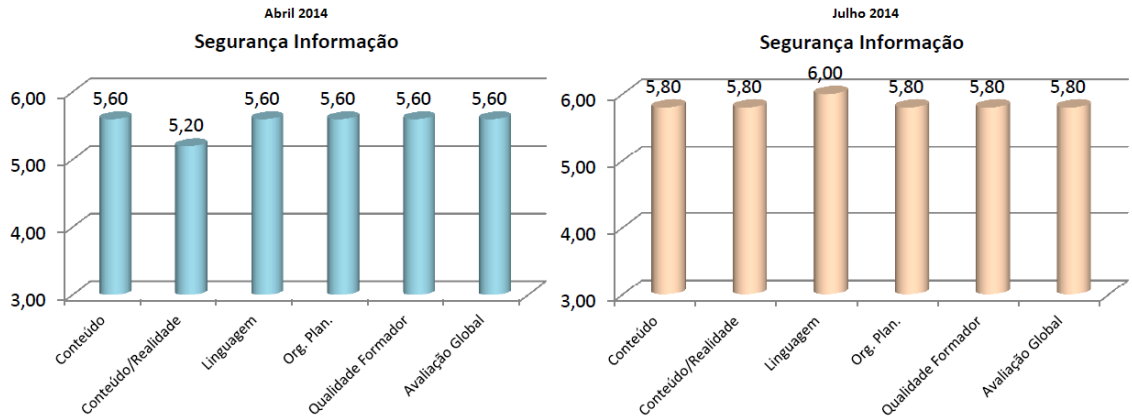
No geral, não se registam diferenças significativas entre os géneros, salvo as que foram identificadas nestes parágrafos.

5. CONCLUSÕES

Verifica-se que, apesar das ameaças de roubos de palavras-chave serem conhecidas, como van Osten (2014) ou Solove (2003) indicam, existe no seio organizacional uma certa descontração na gestão das senhas de acesso.

Não obstante a regulamentação interna indicar que as palavras-chave são confidenciais e não devem ser reveladas a terceiros em nenhuma circunstância, como indicado também no SANS Institute (2014), que indica que as palavras-passe não devem ser inseridas em mensagens de email ou reveladas por telefone nem compartilhadas com ninguém (sejam administrativos, secretárias, gestores, colegas enquanto se está em férias ou membros da família), alguns colaboradores (7%) responderam que já partilharam credenciais de acesso e inclusive quatro respostas indicaram que lhes foi pedido que partilhassem as suas. Embora se reforce que a partilha de palavras-chave não deve ser feita, 13 pessoas indicaram que foi por falta de acessos informáticos atribuídos.

Conforme se pode verificar nos gráficos 2 e 3, verifica-se que o tema da Segurança da Informação não é considerado, pelo menos pelos colaboradores novos que recebem formação de integração, como algo necessário à realidade dos seus trabalhos. Os gráficos apresentam realidades ligeiramente diferentes. Na formação mais antiga, deram inclusive a nota mais baixa da formação sobre Segurança da Informação, com 5,20. Na outra, os formandos deram 5,80 (num máximo de 6) no Conteúdo/Realidade. Apesar das médias das opiniões dos formandos refletirem valores altos, verifica-se que não consideram a Segurança da Informação prioritária ou como de máxima importância para os seus trabalhos.



Gráficos 2 e 3 – Avaliação da Segurança da Informação nas ações de integração (abril de 2014 e julho de 2014)
Fonte: Dados da Seguradora

Um resultado positivo que se extrai dos dados dos inquéritos é a situação de que 71% das pessoas indicam que não utilizam palavras conhecidas para gerarem as suas palavras-passe. De facto, este é um dos temas mais discutidos entre os autores. Segundo uma investigação, 48% das palavras-chave eram baseadas em família (tal como nomes ou datas de aniversário), 33% em diversão (desporto, celebridades), 11% em fantasia e apenas 10% utilizavam efetivamente senhas crípticas, ou seja, difíceis de adivinhar (Brown et al., 2004). Uma outra investigação (Ostojic & Phillips, 2009) indica que 90% dos estudantes universitários utilizam as próprias características para criar as suas credenciais de acesso.

Comparando com os dados do inquérito realizado na seguradora, grande parte das pessoas que responderam que se baseiam em algo para gerar as suas palavras-passe, utilizam nomes de familiares para tal (cerca de 42%). Seguidamente 18 pessoas dizem que utilizam datas especiais como referência para criar senhas. Nota para o facto de que metade das pessoas que indicaram que utilizam nomes de familiares também utilizam outras referências para gerarem palavras-chave. Um dos erros mais comuns ao criar credenciais de acesso é a de colocar simplesmente um ou vários números após uma palavra que se encontra num dicionário (Brown et al., 2004).

Um outro problema detetado é o facto dos colaboradores normalmente utilizarem as mesmas senhas de autenticação para sistemas diferentes, com um resultado positivo nos 57%. Este procedimento acontece, pois é mais fácil de memorizar uma palavra-passe para sistemas diferentes que memorizar várias ou arriscar-se a escrever as mesmas. No entanto, a repetição de senhas é dos maiores erros que um utilizador pode fazer (Brown et al., 2004). Neste caso, se um pirata informático tiver acesso a uma palavra-chave, conseguirá entrar em vários sistemas (Ives et al., 2004), o que faz com que um sistema bem protegido seja tão forte quanto o mais fraco.

Verifica-se que esta seguradora tem estabelecidas algumas regras que grande parte dos autores recomenda que sejam seguidas. As palavras-chave criadas têm que ter no mínimo 8 caracteres, um a mais do que Hitachi (2014) recomenda, mas menos do que as dez que Jacobs (2011) indica, e exatamente o mesmo número que Naik & Sanyal (2012) referem. Brown et al. (2004) escrevem que uma senha de acesso deve ter entre 6 a 8 caracteres.

A seguradora tem uma grande preocupação com a segurança da sua informação, pois a confiança dos clientes diminui em caso de ataques tecnológicos (Dutta &

McCrohan, 2002), embora os colaboradores não correspondam da mesma maneira, conforme verificado pelos resultados do inquérito e das ações de integração.

Conforme muitos autores defendem, se as regras sobre palavras-chave forem mais apertadas, o risco de se abrir falhas na segurança aumenta, através da escrita das mesmas em papéis, onde a segurança resume-se à segurança que o colaborador tem com o papel (Hitachi, 2014) ou da utilização de senhas de autenticação com palavras conhecidas (Campbell et al., 2007), ou mesmo da reutilização de palavras-passe em sistemas diferentes (Pilar et al., 2012). Deste modo, uma das soluções para melhorar esta segurança será consciencializar os colaboradores da organização para que compreendam que este tema não deve ser descuidado (B. von Solms & von Solms, 2004), pois os utilizadores não se protegem se não conhecerem as ameaças e as respetivas consequências. A International Standard Organization (2009) recomenda que as empresas tenham uma política e objetivos de segurança de informação para todo o pessoal, considerado o elo mais fraco, sendo que é necessário que as regras de palavras-chave sejam conhecidas para garantir a integridade da organização (van Osten, 2014).

Uma outra solução, que implica um maior custo para a organização em causa, será a utilização de dois controlos de acesso, como Erdem et al. (2010) defendem, em que se utiliza um smart card que contém todos os usernames e senhas de acesso para o utilizador se autenticar nos sistemas. Essa autenticação seria feita através da inserção do cartão e de um PIN que seria o único código que o colaborador teria que decorar. Neste caso, a organização teria que fornecer um cartão a todos os colaboradores que seria configurado para todos os sistemas em causa, sendo este um dos maiores custos associados.

Uma solução que implicava uma mudança nos documentos da organização seria um single sign-on para todos os sistemas e a alteração das regras de credenciais de acesso para que a mesma seja difícil de adivinhar, sendo que a alteração ocorreria apenas quando se suspeitasse de que a palavra-passe foi comprometida ou a aceitação de que a mesma seja anotada, desde que de um modo seguro (Singer & Anderson, 2013). Esta alteração implica que os responsáveis da companhia aceitem estas novas condições para todos os colaboradores e para toda a organização e percebam os riscos inerentes a este sistema.

Verifica-se então que a seguradora em estudo tem grandes controlos para a mitigação do risco na gestão e utilização das suas palavras-chave, pois vários dos métodos que foram descritos são seguidos pela companhia. Contudo, de modo a

reduzir os riscos existentes, sugere-se que se informe melhor os colaboradores de quais os perigos de se partilharem palavras-passe ou de anotar sem segurança as credenciais de acesso, através de sessões de esclarecimento ou enviando emails informativos.

A utilização de outras formas de autenticação, como aumentar a complexidade das palavras-passe, utilização de tokens ou indicadores biométricos deve ser aplicada apenas para a informação mais sensível que a empresa tenha em sua posse, para evitar que os utilizadores enfraqueçam o sistema de acesso através dos memorandos que pode apontar em qualquer lado.

Seja qual for a solução escolhida para a melhoria da Segurança de Informação, será necessário perceber que não existe uma solução 100% eficaz e que a gestão de risco operacional é uma fonte de sucesso na atividade de uma instituição financeira (Gonçalves, 2011). Como diz Nichols (2000), todas as pessoas correm riscos, mas o utilizador final é o elo mais fraco, independentemente da evolução da segurança tecnológica ("Ending the age of the password," 2005).

6. LIMITAÇÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Este trabalho centrou-se na gestão e utilização de palavras-passe de uma seguradora portuguesa, cujos procedimentos e recomendações foram aqui colocadas. As opiniões dos colaboradores desta empresa sobre estas políticas, bem como os seus modos de geração, memorização e gestão das palavras-passe foram incluídos.

Uma limitação foi o acontecimento de apenas se efetuar a pesquisa numa única empresa seguradora no mercado português, não se sabendo que práticas e procedimentos as outras seguradoras utilizam no seu dia-a-dia. O facto de não se conseguir comparar os métodos de autenticação nesta organização com os métodos recomendados dos autores para mitigação do risco ou mudança de políticas de palavras-chave foi outra barreira que não foi possível superar, mas que seria bastante útil para verificar se tais sugestões seriam práticas e eficazes, ou se pelo contrário, não acrescentam valor relativamente ao processo atual.

Para a realização de trabalhos futuros, recomenda-se:

- Investigar as políticas de gestão de palavras-chaves noutras instituições financeiras, como por exemplo, bancos ou instituições de crédito, ou em organizações que trabalhem com dados sensíveis, como o caso de centros de saúde;
- Fazer uma análise global às políticas de palavras-chave que diversas seguradoras a atuar no mercado português utilizam e verificar as semelhanças e diferenças que têm para a proteção da sua informação. Se possível, estudar o comportamento dos colaboradores das empresas, para verificar se estão dentro das políticas e se tomam cuidados para a proteção da informação;
- Analisar se outro método de autenticação numa organização seria mais eficaz, através da implementação do mesmo, em comparação com o sistema atual na organização em estudo e verificar qual o que os colaboradores preferem ou tomam maiores precauções.

7. BIBLIOGRAFIA

Acar, T., Belenkiy, M., & Küpçü, A. (2013). Single password authentication. Computer Networks, 57(13), 2597-2614. doi: 10.1016/j.comnet.2013.05.007

Almaça, J. A. F. (2010). Xeque à Globalização (Vol. 1). Lisboa: UAL - Universidade Autónoma de Lisboa.

Althaus, C. E. (2005). A Disciplinary Perspective on the Epistemological Status of Risk. Risk Analysis, 25(3), 567-588. doi: 10.1111/j.1539-6924.2005.00625.x

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313. doi: 10.1016/S0167-4048(03)00407-3

Astakhova, L. (2014). The concept of the information- security culture. Sci. Tech.Inf. Proc., 41(1), 22-28. doi: 10.3103/S0147688214010067

Aven, T. (2012). The risk concept-historical and recent development trends. Reliab. Eng. Syst. Saf., 99, 33-44. doi: 10.1016/j.ress.2011.11.006

Aven, T. (2013). On the Meaning and Use of the Risk Appetite Concept. Risk Analysis, 33(3), 462-468. doi: 10.1111/j.1539-6924.2012.01887.x

Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. International Journal of Accounting Information Systems, 13(4), 357-381. doi: http://dx.doi.org/10.1016/j.accinf.2012.03.001

Bernroider, E. W. N., & Ivanov, M. (2011). IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. International Journal of Project Management, 29(3), 325-336. doi: 10.1016/j.ijproman.2010.03.002

Brinkmann, J. (2013). Combining Risk and Responsibility Perspectives: First Steps. J Bus Ethics, 112(4), 567-583. doi: 10.1007/s10551-012-1558-1

Brown, A. S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. Applied Cognitive Psychology, 18(6), 641-651. doi: 10.1002/acp.1014

Burg, D., Compton, M., Harries, P., Hunt, J., Lobel, M., Loveland, M., . . . Schive, L. (2014). US cybercrime: Rising risks, reduced readiness. 19. http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Campbell, J., Kleeman, D., & Ma, W. (2007). The Good and Not So Good of Enforcing Password Composition Rules. Information Systems Security, 16(1), 2-8. doi: 10.1080/10658980601051375

Cantwell, C. (2010). Password Policy for Non-Spine Connected Applications: Good Practice Guideline (pp. 28): NHS.

Castañeda, L. (2012). Alta Gestão nas PME. Porto: Vida Económica.

CEIOPS' Advice for Level 2 Implementiing Measures on Solvency II: SCR standard formula - Article 11 (f) Operational Risk (2009).

Chen, P. Y., Kataria, G., Krishnan, R., & Chen, P.-y. (2011). Correlated failures, diversification, and information security risk management.(Report). MIS Quarterly, 35(2), 397.

Chi-Hsiang Wang, C.-H. W., & Dwen-Ren Tsai, D.-R. T. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization (pp. 265-267).

Cisco. (2014). Cisco 2014 Midyear Security Report (pp. 53): Cisco.

Daniel, L. (2009). ABC dos seguros. Porto: Vida Económica.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 04(02), 92.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87.

Ellwanger, C., Nunes, R. C., Rocha, R. A. D., & Oliveira, M. A. F. (2012). Política de segurança da informação: contribuições do endomarketing para sua efetividade. Revista Produção Online, 12(2), 402. doi: 10.14488/1676-1901.v12i2.887

Ending the age of the password. (2005). Computer Weekly, 30-30.

Erdem, E., Kucukkurt, K. O., Samurkas, K., Kanargi, E., & Celikkan, U. (2010). A smart card based single Sign-On and password management solution as a browser extension (pp. 539-543).

Gillet, R., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. Journal of Banking and Finance, 34(1), 224-235. doi: 10.1016/j.jbankfin.2009.07.020

Gonçalves, R. A. H. (2011). Sistemas de informação para gestão de risco operacional em instituições financeiras. Instituto Superior de Economia e Gestão. Retrieved from http://hdl.handle.net/10400.5/4264

Grob, H. L., Gereon, S., & Buddendick, C. (2008). Applications for IT-Risk Management - Requirements and Pratical Evaluation. Paper presented at the Third International Conference on Avaliability, Realiability and Security.

Haimes, Y. Y. (2009). On the Complex Definition of Risk: A Systems- Based Approach. Risk Anal., 29(12), 1647-1654. doi: 10.1111/j.1539-6924.2009.01310.x

Hitachi. (2014). Password Management Best Practices (pp. 25): Hitachi ID Systems, Inc.

Holton, G. (2004). Defining Risk. Financial Analysts Journal, 60(6), 7.

Hora, M., & Klassen, R. D. (2013). Learning from others' misfortune: Factors influencing knowledge acquisition to reduce operational risk. Journal of Operations Management, 31(1–2), 52-61. doi: http://dx.doi.org/10.1016/j.jom.2012.06.004

Horta, J. (2014). A Gestão (com lucro) da Seguradora (V. Económica Ed.). Porto.

Institute, S. (2014). Password Protection Policy Consensus Policy Resource Community (pp. 4): SANS Institute.

ISACA. (2012). COBIT 5 -A Business Framework for the Governance and Management of Enterprise IT. 94.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. Communications of the ACM, 47(4), 75-78. doi: 10.1145/975817.975820

Jacobs, D. L. (2011). Password Protection. Forbes, 187(6), 62-63.

Jarrow, R. A. (2008). Operational risk. J. Bank Financ., 32(5), 870-879. doi: 10.1016/j.jbankfin.2007.06.006

Leiss, W. (2010). A Note on Yacov Y. Haimes, "On the Complex Definition of Risk". Risk Analysis, 30(7), 1019-1020. doi: 10.1111/j.1539-6924.2010.01396.x

Leitch, M. (2010). ISO 31000:2009-The New International Standard on Risk Management. Risk Anal., 30(6), 887-892. doi: 10.1111/j.1539-6924.2010.01397.x

Luko, S. (2013a). Risk Management Principles and Guidelines. Quality Engineering, 25(4), 451-454. doi: 10.1080/08982112.2013.814508

Luko, S. (2013b). Risk Management Terminology. Quality Engineering, 25(3), 292-297. doi: 10.1080/08982112.2013.786336

Melro, M. F., Fernandes, C. O., & Castro, R. (2007). CobiT 4.1 I. G. Institute (Ed.) (pp. 212).

Merkelsen, H. (2011). The constitutive element of probabilistic agency in risk: a semantic analysis of risk, danger, chance, and hazard. J. Risk Res., 14(7), 881-897. doi: 10.1080/13669877.2011.571781

Naik, P., & Sanyal, S. (2012). Prover and Verifier Based Password Protection: PVBPP.

Nichols, R. W. (2000). Risk. Sci.-New York, 40(3), 4-4.

Organization, I. S. (2009). ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary (pp. 19). Switzerland.

Ostojic, P., & Phillips, J. G. (2009). MEMORABILITY OF ALTERNATIVE PASSWORD SYSTEMS. Int. J. Pattern Recognit. Artif. Intell., 23(5), 987-1004. doi: 10.1142/S0218001409007429

Password savvy.(Living Well: LOOK GOOD, FEEL GOOD.)(Brief article). (2008). Saturday Evening Post, 280(2), 36.

Pilar, D. R., Jaeger, A., Gomes, C. F. A., & Stein, L. M. (2012). Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. PLoS One, 7(12). doi: 10.1371/journal.pone.0051067

Pogue, D. (2011). Password Prevented. Scientific American, 305(3), 36. doi: 10.1038/scientificamerican0911-36

Purdy, G. (2010). ISO 31000: 2009—Setting a New Standard for Risk Management. Risk Analysis, 30(6), 881-886. doi: 10.1111/j.1539-6924.2010.01442.x

Rowan, T. (2009). Password protection: the next generation. Network Security, 2009(2), 4-7. doi: http://dx.doi.org/10.1016/S1353-4858(09)70015-7

Sandhu, R., & Samarati, P. (1996). Authentication, access control, and audit. ACM Comput. Surv., 28(1), 241-243.

Santos, C. I. F. L. B. d. (2013). Implementação de um sistema de informação para gestão de risco operacional numa instituição bancária portuguesa: o caso de estudo. Universidade Nova de Lisboa. Retrieved from http://hdl.handle.net/10362/10514

Santos, D. L. R., & Silva, R. M. S. (2012). Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001. Faculdade de Engenharia - Universidade do Porto.

Savić, A. (2008). Managing IT-related operational risks. Economic Annals, 53(176), 88.

Scarfone, K., & Souppaya, M. (2009). Guide to Enterprise Password Management (Draft). National Institute of Standards and Technology.

Singer, A., & Anderson, W. (2013). Rethinking Password Policies. Usenix, 38(4), 6.

Solove, D. J. (2003). Identity Theft, Privacy, and the Architecture of Vulnerability. Hastings Law Journal, Vol. 54, 46.

Standardization, I. O. f., & Commission, I. E. (2013). Norma Portuguesa - ISO/IEC 27001 (pp. 31).

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events.(Industry overview). Journal of Economic Behavior & Organization, 85, 191.

Thomson, K.-L., & von Solms, R. (2005). Information security obedience: a definition. Computers & Security, 24(1), 69-75. doi: 10.1016/j.cose.2004.10.005

Tiwari, P. B., & Joshi, S. R. (2009). Single sign-on with one time password (pp. 1-4).

Ulloa, A. (2011). A Sociedade da Informação (Vol. 19). Portugal: Planeta deAgostini.

van Osten, C. (2014). Verizon 2014 PCI Compliance Report. In A. Mahaffy, A. DeGuzman, G. Leperlier, I. White, J. Villegas, K. Haverblad, P.-E. Leriche, P. Grobler, R. Dolado, R. van Koten, & R. Tosto (Eds.), (pp. 56): Verizon Enterprise Solutions.

Verizon. (2013). 2013 Data Breach Investigations Report (pp. 63): Verizon.

Vilares, M. J., & Simões Coelho, P. (2011). Satisfação e Lealdade do Cliente. Lisboa: Escolar Editora.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. doi: 10.1016/j.cose.2004.05.002

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. doi: 10.1016/j.cose.2013.04.004

Yin, R. K. (2009). Case Study Research: Design and Methods (Fourth Edition ed. Vol. 5). Thousand Oaks, California: SAGE Publications.

Yongzhong, H., & Zhen, H. (2009). User Authentication with Provable Security against Online Dictionary Attacks. Journal of Networks, 4(3), 200.

Zsidisin, G. A. (2003). A grounded definition of supply risk. Journal of Purchasing and Supply Management, 9(5), 217-224. doi: 10.1016/j.pursup.2003.07.002

8. ANEXOS

8.1. INQUÉRITO

Geral

Género

M

F

Idade

(Escrever idade)

Departamento

Financeiro e Planeamento

Sinistros

Técnica e Atuariado

Comercial

Informática

Institucional

Outros (CEO, Auditoria, Jurídico, Marketing, Secretariado, Recursos Humanos, Internacional)

Há quanto tempo trabalha na Seguradora?

Menos de um ano

Entre 1 a 3 anos

Entre 4 a 9 anos

Entre 10 a 20 anos

Mais de 20 anos

Sobre Passwords

Quantas passwords utiliza na Seguradora?

1

2

3

Mais de 3

Utiliza as mesmas passwords para sistemas diferentes, sempre que possível?

Sim

Porque motivo utiliza as mesmas passwords para sistemas diferentes?

Mais fácil de memorizar

Penso que é o procedimento mais correto

Outro

Não

Porque motivo não repete as passwords em sistemas diferentes?

Acho que é o melhor procedimento

Preocupo-me com a segurança da informação

Outro

Anota as suas passwords para não se esquecer?

Sim

Como anota as suas passwords?

Múltipla escolha

Num post-it, que colo no monitor

Num papel, que fica debaixo do teclado

Coloco o papel numa gaveta

Escrevo em código

Anoto no telemóvel

Escrevo num notepad do computador

Outro

Não

Qual a sua opinião sobre as políticas de password na Seguradora?

Múltipla escolha

São muitas passwords para decorar

Têm muitas regras para cumprir

Acredito que deste modo está bom

Penso que as regras deveriam ser mais apertadas

Que tal mudar para outro sistema (Cartão, indicador biométrico, ...)?

Outro

Partilha de passwords

Já lhe foi solicitado que partilhasse passwords

Sim

Quantas vezes é que lhe foi solicitado?

1 vez

2 vezes

Mais de 2 vezes

Não

Já partilhou alguma password sua com colegas?

Sim

Quantas vezes partilhou passwords?

1 vez

2 vezes

Mais de 2 vezes

Foi por sua iniciativa que partilhou passwords?

Sim

Não

Foi para mais que um sistema que partilhou passwords?

Sim

Não

Porque motivo partilhou passwords?

Múltipla Escolha

Férias

Baixa/doença
Falta de acessos atribuídos
Outro

Depois da partilha, mudou a password?
Sim
Não

Não

Qual é a sua opinião sobre a partilha de passwords?
1 (Sem gravidade)
2
3
4
5 (Muito grave)

Se eu partilhar uma password minha com um colega e este fizer algo grave, o ónus será:
Dele, pois foi ele que trabalhou no sistema
Dele, pois tenho um email a indicar que lhe partilhei a password
Meu, pois fui eu que partilhei a password
Meu, pois o sistema anota que o meu userID fez o trabalho

Passwords - Sistema Windows

Muda a sua password apenas quando o sistema obriga-o a tal?
Sim
Não

Quando é que altera a sua password?
Altero quando o sistema diz que tenho de alterá-la em X dias
Altero à minha medida, antes do sistema avisar

Quando muda de password, muda apenas um carácter?
Sim
Não

Utiliza, dentro do possível, palavras conhecidas?
Sim

Utiliza que género de palavras para criar as suas passwords?
Múltipla escolha
Nomes de familiares
Locais e/ou países
Datas de eventos
Nomes de animais de estimação
Personagens de ficção
Títulos de músicas, livros ou filmes
Outro

Não

Por norma, quantos requisitos cumprem as suas passwords?
3 (mínimo pedido)
4

Ao fim de 12 passwords diferentes para entrar no Windows, volta a utilizar as mesmas passwords?

Sim

Não

Não se aplica

Não me lembro

8.2. RESPOSTAS

8.2.1. Geral

Género	
Masculino	Feminino
166	139
54%	46%

Departamento						
Financeira e Planeamento	Sinistros	Técnica e Atuariado	Comercial	Informática	Institucional	Vários
29	48	31	150	22	6	19
10%	16%	10%	49%	7%	2%	6%

Tempo de casa				
Menos de 1 ano	Entre 1 a 3 anos	Entre 4 a 9 anos	Entre 10 e 20 anos	Mais de 20 anos
25	46	107	76	51
8%	15%	35%	25%	17%

Número de passwords			
1	2	3	Mais de 3
23	67	88	127
8%	22%	29%	42%

Idade				
[20-30[	[30-40[	[40-50[	[50-65]	Inválidas
43	113	87	61	2
14%	37%	28%	20%	1%

8.2.2. Sobre passwords

Utiliza as mesmas passwords para sistemas diferentes, sempre que possível?	
Sim	Não
175	130
57%	43%

Porque motivo utiliza as mesmas passwords para sistemas diferentes?		
Mais fácil de memorizar	Penso que é o procedimento mais correto	Outro
155	9	11
89%	5%	6%

Porque motivo não repete as passwords em sistemas diferentes?		
Acho que é o melhor procedimento	Preocupo-me com a segurança da informação	Outro
40	77	13
31%	59%	10%

Anota as suas passwords para não se esquecer?	
Sim	Não
111	194
36%	64%

Qual a sua opinião sobre as políticas de password na Seguradora?	
Muitas Passwords para decorar	80
Muitas regras para cumprir	62
Deste modo está bom	139
Mudar de sistema	96
As regras deveriam ser mais apertadas	3
Oito caracteres num telemóvel é exagero	1
Sugerem uma única password para todos os sistemas, eventualmente que expirasse mais rapidamente	3

8.2.3. Partilha de passwords

Já lhe foi solicitado que partilhasse passwords?	
Sim	Não
4	301
1%	99%

Quantas vezes é que lhe foi solicitado?		
1 vez	2 vezes	Mais de 2 vezes
1	0	3
25%	0%	75%

Já partilhou alguma password sua com colegas?	
Sim	Não
21	284
7%	93%

Quantas vezes partilhou passwords?		
1 vez	2 vezes	Mais de 2 vezes
9	2	10
43%	10%	48%

Foi por sua iniciativa que partilhou passwords?	
Sim	Não
18	3
86%	14%

Foi para mais que um sistema que partilhou passwords?	
Sim	Não
0	21
0%	100%

Por que motivo partilhou passwords?			
Férias	Baixa / Doença	Falta de acessos atribuídos	Outro
5	0	10	8
22%	0%	43%	35%

Depois da partilha, mudou a password?	
Sim	Não
17	4
81%	19%

Qual é a sua opinião sobre a partilha de passwords?				
1	2	3	4	5
5	5	22	72	201
2%	2%	7%	24%	66%

Se eu partilhar uma password minha com um colega e este fizer algo grave, o ónus será:			
Dele, pois foi ele que trabalhou no sistema	Dele, pois tenho um email a indicar que lhe partilhei a password	Meu, pois fui eu que partilhei a password	Meu, pois o sistema anota que o meu userID fez o trabalho
3	0	198	104
1%	0%	65%	34%

8.2.4. Passwords – Sistema Windows

Muda a sua password apenas quando o sistema obriga-o a tal?	
Sim	Não
291	14
95%	5%

Quando é que altera a sua password?	
Altero quando o sistema diz que tenho de alterá-la em X dias	Altero à minha medida, antes do sistema avisar
4	10
29%	71%

Quando muda de password, muda apenas um caracter?	
Sim	Não
171	134
56%	44%

Utiliza, dentro do possível, palavras conhecidas?	
Sim	Não
87	218
29%	71%

Por norma, quantos requisitos cumprem as suas passwords?	
3 (mínimo exigido)	4
195	110
64%	36%

Ao fim de 12 passwords diferentes para entrar no Windows, volta a utilizar as mesmas passwords?			
Sim	Não	Não se aplica	Não me lembro
28	160	32	85
9%	52%	10%	28%

8.2.5. Respostas abertas

Porque motivo utiliza as mesmas passwords para sistemas diferentes?	
Mais fácil de memorizar	156
Procedimento mais correto	9
Evitar cábulas; facilidade	3
Muitas plataformas sem single sign-on	1
Obrigatoriedade de sistemas	2
Usam passwords diferentes (erro)	4

Porque motivo não repete as passwords em sistemas diferentes?	
Acho que é o melhor procedimento	40
Preocupação com Segurança da Informação	77
Não confundir	1
Regras diferentes nos diversos sistemas	8
Alterações em momentos diferentes	2
Sem Critério	1
Usam passwords iguais (erro)	1

Como anota as suas passwords?	
Agenda particular	8
Telemóvel	16
Notepad/Excel do Computador	12
Papel numa gaveta	28
Aplicações próprias	7
Escrita em código	28
Registada fora da companhia	2
Debaixo do teclado	2
Num bloco	7

Qual a sua opinião sobre as políticas de password na Seguradora?	
Muitas Passwords para decorar	80
Muitas regras para cumprir	62
Deste modo está bom	139
Mudar de sistema	96
As regras deveriam ser mais apertadas	3
8 caracteres num telemóvel é exagero	1
Sugerem uma única password para todos os sistemas, eventualmente que expirasse mais rapidamente	3

Por que motivo partilhou passwords?	
Falta de acessos	13 (3 reclamam urgência)
Ausência	5
Informática (a pedido de)	2
Telemóvel	1

Utiliza que género de palavras para criar as suas passwords?	
Nomes	39
Datas	18
Animais	8
Títulos	8
Nomes de familiares e outras referências	19
Outras referências (não especificado)	19